Table of Contents

LevelBlue Managed Security Services

Section Effective Date: 01-Oct-2014

The LevelBlue Managed Security Services portfolio is a selection of security services that includes managed Premises-Based Firewall, Intrusion Detection and Prevention, Proxy, Token Authentication, and Distributed Denial of Service.

The LevelBlue Managed Security Services Service Guide consists of the following parts:

- Service Description (SD)
- Service Level Agreements/Service Level Objectives (SLA/SLO)
- Pricing (P)
- Country Specific Provisions (CSP)

In addition, the General Provisions are incorporated and apply as specified therein.

Service Description (SD)

SD–1. General

SD–1.1. LevelBlue Managed Security Service

Section Effective Date: 17-Nov-2025

The following table describes at a high level the applicable capabilities for each of the managed security services described in this guide.

Managed Security Services Capabilities			
Managed Service	**Architecture Summary and Options**	**Key Features**	**Reporting**
LevelBlue Premises-Based Firewall	Premises-Based Firewall is fully managed by LevelBlue from highly secure and redundant Security Operation Centers (SOCs). Custom network security policy is applied and is able to be changed. Firewalls inspect each packet and allow or deny it. Event logs are analyzed to issue alerts if suspicious activity is detected. The service is available in multiple levels of configuration; Essential, Standard, Premium and Enterprise.	-Fully Managed Solution –Fully provisioned firewall solution. -Proactive monitoring- 24x7 from the LevelBlue Security Operation Centers (SOCs). -Constant analyses against known vulnerabilities and threats. -Patches and maintenance included.	LevelBlue Portal

Managed Security Services Capabilities			
Managed Service	**Architecture Summary and Options**	**Key Features**	**Reporting**
Managed Intrusion Detection/ Prevention System (MIDPS)	Monitors a Customer network via an unaddressed monitor port on a switch at your premises. Highly secure Intrusion Detection Sensors located at your site use a signature-based approach to perform intrusion detection at the network level. When a pattern of misuse is detected, the system quickly and automatically responds according to Customer's pre-defined policies to send an alert and take immediate action	-Security Network Operations Center -Customer- defined Signature Creation and Security Posture Customization -On-site installation and maintenance -Incident response -Perimeter Intrusion Detection	Interactive reporting through LevelBlue Security Center Portal on each S/NOC managed intrusion detection sensor.
LevelBlue Proxy Service (APS)	APS consists of a proxy server and software proxy appliances that redirect Internet-based traffic through the service. External users who want to access a Customer's resources connect to the proxy server to make the requests. The proxy server evaluates each request, blocking and filtering threats or unauthorized traffic. Controls Internet access for Customer's internal users, mediating their traffic through Customer's URL filtering policy (available as an optional feature).	-Detailed traffic and threat analysis of MPLS routers -Holistic view of MPLS routers -Customizable policy and alerting -Detect worms, scans, zero-day events, darknets, DoS attacks, protocol misuse, phishing attacks, and others -Global security threats feed	Reporting via a portal

Managed Security Services Capabilities			
Managed Service	**Architecture Summary and Options**	**Key Features**	**Reporting**
LevelBlue Private Internet Protect (PIP)	PIP collects and analyzes Internet and Intranet traffic. The controllers analyze the data using heuristics and statistical models designed to predict and profile potential malicious activity. LevelBlue analysts then research the possible cause(s), assess the severity of the anomaly, and decide what action, if any, should be taken. If the LevelBlue analyst determines the severity to be high, an alert is sent via email.	- Private Web Portal - Predictive and early warning about network traffic - Threat Analysis to identify anomalies reflecting known attacks or threats that may warrant imminent attention. - Early intelligence gathering - Expert advice on what to do and how to do it quickly. - Customizable Features - customize policies and alert classification & notification	Reporting via the Security Center portal

Managed Security Services Capabilities			
Managed Service	**Architecture Summary and Options**	**Key Features**	**Reporting**
Distributed Denial of Service (DDoS)	DDoS Defense for AT&T Dedicated Internet (ADI)/ADI+/AT&T Dedicated Internet Global (ADIG) (formerly known as LevelBlue Managed Internet Service (MIS)/MIS+/Global Managed Internet Service (GMIS)) respectively, customers and LevelBlue IDC Hosting customers with connectivity to the LevelBlue IP Backbone	-Volumetric attack detection and mitigation -Reporting portal -24x7 monitoring -No Customer-premises equipment required	Yes
LevelBlue Secure E-Mail Gateway	Email Security	-Customer Managed Administration -Anti-Virus Protection -Spam Filtering -Policy Enforcement -Quarantine -Disaster Recovery -Transport Layer Security -Administrative Reports	Through LevelBlue Portal. For details see reporting section at the end of this Service Guide
Token	Hard or soft tokens for issue to approved users who then access the service via the Internet (Internet access is required)	-Two-Factor Authentication -Usage Reports -LevelBlue Internet Data Centers (IDCs) -Fully Managed Service	Monthly usage and management information reports sent via email.

SD-1.1.1. Reporting through LevelBlue Portal – View Managed Security Reports

Section Effective Date: 17-Nov-2025

Standard reporting is included via LevelBlue's designated portal. Report types are subject to change and are dependent upon device capability and configuration.

SD-1.1.2. Customer Compliance Responsibilities

SD-1.1.2.1. Monitoring of Communication

Section Effective Date: 04-Dec-2019

LevelBlue is providing these Services for a cybersecurity purpose as defined in and consistent with the Cybersecurity Information Sharing Act of 2015 ("CISA"). In the United States, Customer agrees to undertake any monitoring of its network, undertake defensive measures, and share cyber threat indicators or defensive measures consistent with CISA. In the U.S and globally, Customer agrees that it is responsible for setting all security policies, including monitoring policies, and will implement any and all security policies pursuant to CISA or other applicable law. LevelBlue retains the right to reject any security policies Customer asks it to implement that in LevelBlue's sole judgment are not for a cybersecurity purpose or as defined in or are inconsistent with CISA or other applicable law. Customer consents to the monitoring by the Services contemplated here. Customer is responsible for obtaining consent from and giving notice to its Users, employees, and agents regarding Customer's and LevelBlue's collection and use of the User, employee, or agent information in connection with a Service.

SD-1.2. Opt-Out Clause

Section Effective Date: 14-Apr-2022

The Opt-Out Clause applies to the following Managed Security Services:

- LevelBlue Premises-Based Firewall Service
- LevelBlue Intrusion Detection / Prevention Services
- LevelBlue Intrusion Detection / Prevention Services – Host-Based LevelBlue Proxy Services

The Opt-Out Clause applies to Customer's Initial Order ("Initial Order") placed at contract signing in the Service Agreement. Service or features added after Initial Order will be considered change orders and no Opt-Out applies.

Termination Charges and Minimum Payment Periods shall not apply if Customer terminates a Service under the Pricing Schedule Initial Order within thirty (30) days after the Service test and turn-up is completed by LevelBlue and Service has been made available for Customer ("Opt-out Period"). Customer will be required to remit payment for all charges incurred for the Service received.

SD-2. Service Overview – Premise-Based Firewall

Section Effective Date: 02-Mar-2017

LevelBlue Premises-Based Firewall Service ("the Service") is a customer premise installed security service which provides firewall protection to the customers' network connectivity. The fully managed service includes an installed premises-based firewall device, or devices, pre-configured for the Customer's location, fault management, incident management and change management.

LevelBlue Premise-Based Firewall Service supports multiple types of Internet connections on an agnostic basis, including, but not limited to, AT&T Dedicated Internet (ADI) (formerly known as LevelBlue Managed Internet Service (MIS)) and VPN Service Customers.

SD-2.1. Premises-Based Firewall Service Configurations

Section Effective Date: 10-Jan-2017

Premise-Based Firewall Service is available in multiple levels of configuration – Essential, Standard, Premium and Enterprise.

Unless specifically stated herein, the components, features and capabilities of the Enterprise configurations are not applicable to the Essential, Standard and Premium configurations.

SD-2.2. Service Components – Essential and Standard

Section Effective Date: 10-Jan-2017

Installed Premises based firewall device pre-configured for the Customer's location. The pre-configured Premise based firewall device is LevelBlue Equipment. Upon termination or expiration of the Agreement, Customer must properly package, ship and return all LevelBlue Equipment. Failure to do so may result in additional Charges.

SD-2.3. Service Features – Essential and Standard

SD-2.3.1. IPsec VPN Tunneling

Section Effective Date: 23-May-2016

The Service supports use of IPSEC tunneling. IPSEC tunnels transport traffic in an encrypted mode from the customer's site or network to customer designated third parties and suppliers. IPsec support also allows Customer remote users to connect in a highly secure manner to the customers' internal network resources via the managed firewall.

SD-2.3.2. DMZ and Extranet support

Section Effective Date: 23-May-2016

The Service supports use of the remaining physical interfaces within the supplied appliance for use in the creation of DMZ or Extranet interfaces.

SD-2.3.3. Integration Capability with LevelBlue Cloud Web Security Service

Section Effective Date: 23-May-2016

Integration capability with LevelBlue Cloud Web Security Service set forth in the following Service Guide:
http://serviceguidenew.att.com/sg_CustomPreviewer?attachmentId=00P1A00000pWsEjUAK

SD-2.3.4. Fault and Incident Management

Section Effective Date: 23-May-2016

An LevelBlue security analyst will triage security alerts and faults that are generated by the managed device. If the faults or incidents are deemed to be actionable, LevelBlue will engage the customer security contact.

SD-2.3.5. Change Management

Section Effective Date: 23-May-2016

LevelBlue will perform all necessary standard configuration and policy changes to the security technology, based on a mutually agreed upon maintenance window. Changes required as a result of a security event rather than a customer request will be handled in a timely manner. LevelBlue requires Change Requests to be submitted for any customer network modifications in order to maintain service continuity.

SD-2.3.6. Log Data

Section Effective Date: 23-May-2016

Standard Event Retention Policy- All logs are stored in active form for ninety (90) days with offline access for one year.

SD-2.3.7. Reporting and Administrative Portal

Section Effective Date: 10-Jan-2017

Standard reporting is included via LevelBlue's designated portal (not Business Direct for the Essential, Standard or Premium configurations). Report types are subject to change and are dependent upon device capability and configuration.

SD-2.3.8. Onsite Technician Install

SD-2.3.9. Consulting Hour

Section Effective Date: 10-Jan-2017

Unless otherwise set forth in the executed pricing schedule, to assist the Customer with the technical elements of their managed solution during the delivery or operational phase of the engagement, the Customer can purchase LevelBlue Consulting Hours to support their needs beyond the scope of this engagement. Additional hours can be purchased over the term of the engagement. Hours may only be used during the term of contract for the engagement of the Service managed solution.

SD-2.3.10. Fortinet Software-Defined Wide Area Network (SD-WAN) Management

Section Effective Date: 09-Mar-2021

As part of Premise-Based Firewall management services, LevelBlue will manage Fortinet Premise-Based Firewall and Fortinet SD-WAN policy on behalf of the Customer.

SD-2.3.10.1. Fortinet SD-WAN Standard Features

Section Effective Date: 09-Mar-2021

- Application Aware – support for application aware policies and monitoring.
- Quality of Service (QoS) – supports application prioritization.
- Policy Based Traffic Shaping – supports bandwidth minimums and maximums
- IPSec Tunnel – supports the following topology: hub and spoke, and Advanced Virtual Private Network (ADVPN), a dynamic branch-to-branch tunnel.
- Routing Features – Supports Internal Border Gateway Protocol (iBGP) for ADVPN networks.
- Network IP Address Services – supports IPv4 addressing, Dynamic Host Configuration Protocol (DHCP) client, DHCP server, Network Address Translation (NAT).
- Link steering is automatically performed on-demand and is based on configuration of the defined SD-WAN policy.
- Forward Error Correction (FEC) – Applies remediation techniques to correct link degradation (FortiGates to FortiGates only).
- Load Balancing and Bandwidth spill-over – supports traffic management over multiple access types.

SD-2.3.10.2. Management of Fortinet SD-WAN Service

Section Effective Date: 09-Mar-2021

Management functions consist of the following:

SD-2.3.10.2.1. Monitoring and Management

Section Effective Date: 09-Mar-2021

LevelBlue provides monitoring and management of the Fortinet SD-WAN Service, which includes monitoring and troubleshooting of the Service. LevelBlue will make necessary changes to the SD- WAN policy based on Customer requirements and direction.

SD-2.3.10.2.2. Fault Management

Section Effective Date: 09-Mar-2021

LevelBlue provides fault management of the Fortinet SD-WAN Service which includes the following:

- Fault monitoring
- Trouble isolation and resolution
- Issue tracking via Trouble Ticket
- Interfacing with the vendor, as needed

SD–2.3.10.2.3. Maintenance

Section Effective Date: 17-Nov-2025

LevelBlue provides the following life-cycle maintenance, monitoring, and support functions of the Fortinet SD-WAN Service:

- 7-days-per-week, 24-hours-per-day (7 x 24) monitoring of provided Service Components
- Help desk support
- Coordination, as needed, with the vendor in the event of a disruption or a degradation of Service performance
- Ongoing maintenance updates to LevelBlue Equipment in accordance with LevelBlue's maintenance schedule
- Problem management, including logging, tracking, and escalating reported problems based on severity levels, as well as dispatch of and problem diagnosis by maintenance personnel
- LevelBlue maintenance support does not include Sites where notification has been given to Customer that LevelBlue Equipment can no longer be maintained and there is no comparable replacement or Customer does not accept a replacement. In the event the LevelBlue Equipment fails at a Site, and it cannot be repaired, Service will be disrupted until the Customer issues a request to change or disconnect the Service. Monthly recurring charges will continue until such time as the Customer requests a change or disconnect, subject to standard timeframes to implement that request.
- Customers can submit a Trouble Ticket to the designated LevelBlue Portal
- LevelBlue will use commercially reasonable efforts to notify Customers in advance of scheduled maintenance periods, repair, or upgrade. LevelBlue reserves the right to perform emergency maintenance as may be required without notice.

SD–2.4. Service Components – Premium

Section Effective Date: 23-May-2016

The Premium Service includes the Standard configuration offering above, including features, and the following additional components.

SD–2.4.1. Intrusion Detection and Prevention

Section Effective Date: 24-May-2016

Intrusion Detection or Prevention (IDP) is a managed attack recognition and response solution for network security. IDP provides Customer with the following standard capabilities.

- Configured IDP in promiscuous mode. Promiscuous mode provides an unobtrusive "sniffing" of traffic via a sensor with logging of suspected or traffic signatures when detected.
- LevelBlue tuned database of intrusion detection signatures on managed devices.

SD–2.5. Customer Care Technical

Section Effective Date: 23-May-2016

Customer Care/Technical Support is available 24 x7 to Customers through their designated points of contact by calling a toll-free (or paid) global service support telephone number.

A “Trouble Ticket”, defined as the individual incident report LevelBlue opens for each outage or other issue with the MSS, will be opened for each incident. The Trouble Ticket begins when the LevelBlue Security Network Operations Center (SNOC) has acknowledged and validated an LevelBlue problem, and when an LevelBlue generated ticket is opened. A Trouble Ticket resolution is defined when the incident is resolved to the satisfaction of both the Customer and LevelBlue and the Trouble Ticket is closed.

Cross References

SD-2.8.11. Ownership

SD–2.6. Acceptable Use

Section Effective Date: 24-May-2016

Subscribers shall not use the Service for any purpose other than as expressly authorized herein.

SD–2.7. Country Availability (Specific to Standard and Premium)

Section Effective Date: 23-May-2016

LevelBlue Premises-Based Firewall Service is available in the United States as noted in the table below.

Table of Regions	
Region	**Countries within a Region**
United States	United States

SD–2.8. Standard Components of the Premises Based Firewall Service – Enterprise

Section Effective Date: 23-May-2016

- 7x24 filtering of traffic through the Firewall running on hardware platforms. Standard outbound Customer security policy allowing all identified Customer internal networks to access all HTTP, HTTPS, and FTP sites.
- User-defined “rule elements” or “rules” that describe how the MFS-PB firewall processes traffic, which types of traffic should be accepted or denied, and which traffic should generate logs for subsequent analysis.
- Stateful Inspection of allowed IP traffic.
- Out-of-band access (via Customer provided POTS line) to a separate control device (LevelBlue supplied) for remote event mitigation and device control capabilities.
- A link back to the SNOC for monitoring access into the MFS-PB firewall.
- Customer defined rules for Internet traffic sent or received by groups of user.
- Network Address Translation (NAT) for internal IP aliases.
- Generation of firewall log data based on the Customer data traffic.
- If User Authentication is requested by Customer, interface between MFS-PB and Customer hosted and managed User Authentication service to authenticate User activity to the Internet. Customer will remain responsible for the provisioning, administering, support and/or troubleshooting of its User Authentication solution.
- Standard MFS-PB reporting.

SD–2.8.1. Optional Components

Section Effective Date: 24-May-2016

The following table describes the optional services available for purchase by the Customer as a part of Premise Based Firewall Service (MFS-PB), and the levels that apply to each:

Features	Description
Advanced Secure Interfaces (ASI)	Provides configuration, maintenance, and management of the MFS-PB settings for additional DMZ or Extranet interfaces. The number of DMZs and Extranets is based on the number of available, native hardware interfaces. By default, MFS-PB includes one DMZ/Extranet interface.
Site-to-Site VPN Support (S2S)	Provides support for the creation of Site-to-Site VPN tunnels permitting clients to connect directly with their parties. The number of tunnels permitted is based on the capacity and throughput of the hardware.
Client-to-Site VPN Support (C2S)	Provides support of Client-to-Site VPN tunnels. Quantity of client tunnels supported is based on the capacity of the installed hardware platform.
Complex Environment (CXE)	Provides support for complex levels of security policies, routing architectures, and firewall Object management.
HA Gateway Architecture	Includes two firewalls and necessary switches to permit active/passive failover configuration
Unified Threat Management (UTM)	See below
Next Generation (NG) Component	See below

SD–2.8.2. Unified Threat Management (UTM) Component

Section Effective Date: 24-May-2016

UTM is available with certain MFS-PB offerings which are subject to change and provides additional features beyond standard firewall capabilities. IN particular, UTM offers: (i) intrusion Detection or Prevention; (ii) Web Filtering; and (iii) Anti-Virus Screening.

SD–2.8.2.1. UTM Intrusion Detection or Prevention (IDP) Option

Section Effective Date: 01-Oct-2014

IDP is a managed attack recognition and response capability for network security. IDP provides Customer with the following standard capabilities:

- Configured IDP in promiscuous mode. Promiscuous mode provides an unobtrusive "sniffing" of traffic via a sensor, with logging of suspended or traffic signatures when detected.
- LevelBlue tuned database of intrusion detection signatures on managed UTM devices.
- IDP reporting via the LevelBlue Security Center Portal
- 24x7 Investigative Phone Support
- Incident Notification

Customer may purchase the following additional IDP options:

Features	Description
Enhanced Threat Segments (ETS)	Each IDP offer includes one monitored segment. Additional segments may be monitored by the inclusion of the ETS option and are available for purchase on a per segment basis.
Advanced Threat Solutions (ATS)	ATS includes: High Severity alerts also include phone call to security contact. Two weeks profiling – Provide profiling (enhanced tuning and data traffic analysis) to give a baseline of the customer network or Host alarm activity, including analysis and verification by LevelBlue. Continuous sensor tuning based on Customer environment. Custom Signatures – 20 concurrent custom signatures per client. Root Cause Analysis associated with High Level Alerts.

SD-2.8.2.2. UTM Web Filtering Option

Section Effective Date: 17-Nov-2025

The UTM Web Filtering option provides Customer with the ability to allow or block access to Internet websites by category, blacklist, whitelist and source IP. In particular, the Web Filtering option includes:

- Applied default LevelBlue URL/Web Filtering (URL/WF) policy on managed UTM devices
- Updated URL/WF database
- URL/WF changes via Customer initiated MACD request via the LevelBlue Portal
- URL/WF reporting via the LevelBlue Security Center portal
- Support of LDAP integration for user/group specific filtering policy

SD-2.8.2.3. UTM Anti-Virus Option

Section Effective Date: 01-Oct-2014

The UTM Anti-Virus option provides an anti-virus filtering process that is designed to detect, clean, and record virus infected traffic before it enters the Customer network. The Anti-Virus option can be configured to scan all inbound and outbound traffic for viruses and utilizes virus definition libraries that are updated with new virus signatures. The Anti-Virus option includes a default anti-virus policy on the managed firewall device.

SD-2.8.3. Next Generation (NG) Component

Section Effective Date: 24-May-2016

The NG component is available with certain MFS PB firewall offerings, which are subject to change, and provides additional features to Customer beyond standard firewall capabilities. In particular, NG offers: (i) Application Awareness; (ii) Intrusion Detection or Prevention; (iii) Web Filtering; and (iv) Anti-Virus Screening.

SD–2.8.3.1. Application ID Aware Firewall

Section Effective Date: 01-Oct-2014

Enable the configuration:

- Configuration is operational 24x7
- Configuration acts upon applicable candidate traffic based upon Customer-defined rule base
- Download and install standard libraries delivered on a weekly basis from the application identification system

SD–2.8.3.2. Customer Read–Only Access and Reporting

Section Effective Date: 17-Nov-2025

Enable appliance configuration to provide up to three (3) authorized Customer security contacts with locally authenticated Read-Only access to the managed device to permit the following:

- View Customer-defined firewall policy rule-base and device configuration
- View active log files from system functions
- Support configuration of appliance to automate delivery of pre- defined reports to Customer defined receivers on a daily/weekly/monthly schedule as the device permits.
- Create custom application definitions based upon sufficient information obtained from the authorized Customer security contact.

SD–2.8.4. Zero Day Malware Detection System (ZDMDS) Option

Section Effective Date: 24-May-2016

ZDMDS is designed to enable end-users to automatically identify and protect against new and unknown malware entering their network.

- Enable the Configuration
- Configuration is operational 24x7
- Configuration acts upon applicable candidate traffic based upon Customer-defined rule base
- Device uploads potentially malicious files to the malware detection system for analysis
- Configuration updates from the signature generation system for globally detected previously unknown zero hour malicious signatures
- Appropriate action of the managed appliance based on library updates

SD–2.8.5. Web Filtering Option

Section Effective Date: 24-May-2016

The Web Filtering option provides Customer with the ability to allow or block access to Internet web sites by category, blacklist, whitelist, and source IP. In particular, the Web Filtering option includes:

- Applied default LevelBlue URL/Web Filtering (URL/WF) policy on managed devices
- Updated URL/WF database
- URL/WF changes via Customer initiated Move, Add, Change and Delete (MACD) request via the LevelBlue BusinessDirect Portal.

SD–2.8.6. Threat Protection Option

Section Effective Date: 24-May-2016

- Anti-Virus: The Anti-Virus feature provides an anti-virus filtering process that is designed to detect, clean, and record virus infected traffic before it enters the Customer network. The Anti-Virus feature can be configured to scan all inbound and outbound traffic for viruses and utilizes virus definition libraries that are updated with new virus signatures. The Anti-Virus option includes a default anti-virus policy on the managed firewall device.
- Intrusion Detection or Prevention: Intrusion Detection or Prevention (IDP) is a managed attack recognition and response solution for network security. IDP provides Customer with the following standard capabilities.
- Configured IDP in promiscuous mode: Promiscuous mode provides an unobtrusive "sniffing" of traffic via a sensor with logging of suspected or traffic signatures when detected.
- LevelBlue tuned database of intrusion detection signatures on managed devices
- 24x7 Investigative Phone Support
- Incident Notification
- High Severity alerts also include phone call to security contact
- Two week profiling – Provide profiling (enhanced tuning and data traffic analysis) to give a baseline of the Customer network or Host alarm activity, including analysis and verification by LevelBlue.
- Continuous sensor tuning based on Customer environment
- Custom Signatures – Twenty (20) concurrent custom signatures per client
- Root Cause Analysis associated with High Level Alerts

Customer will also have the ability to purchase the following additional IDP options

Features	Description
Enhanced Threat Segments (ETS)	Each IDP offer includes one monitored segment. Additional segments may be monitored by the inclusion of the ETS option and are available for purchase on a per segment basis.

SD–2.8.7. Customer Responsibilities

Section Effective Date: 21-Nov-2017

To manage the Services outlined herein for the Charges set forth below, Customer is assigned roles and responsibilities must be fulfilled effectively. Customer is responsible for the following:

SD–2.8.7.1. Customer Responsibilities for Managed Security Services (MSS)

Section Effective Date: 21-Nov-2017

- Designate Customer Site Security Liaison who will be the technical focal point to work with LevelBlue to help promote a successful implementation.
- Provide a Site contact who will participate in installation and troubleshooting (as deemed necessary by LevelBlue), and who will conduct pre-installation and post-installation User Acceptance Testing (UAT).
- Provide a Tier 1 Helpdesk
- Review and provide relevant comments (in the form of additional data requirements, preliminary conclusions, or recommended technical architecture) or Subject Matter Experts (SME) resources from applicable information technology departments or business units to assist in completing LevelBlue deliverables in a timely manner.
- Ensure LevelBlue access to the Customer Site to maintain LevelBlue-provided hardware and software. Should LevelBlue be denied access at a Site, the Customer will incur the applicable rescheduling Charges.
- Perform Site preparation including, but not limited to, heating, ventilation, air conditioning, electricity, cabling, entrance facilities and demarcation extensions.
- Provide space, racks, connectors, and suitable environment for the LevelBlue CPE, as specified by the manufacturer.
- Notify LevelBlue in advance about planned changes to Customers' network configuration(s). Required changes that result from these notifications may incur a conversion Charge for affected MSS components.
- Notify LevelBlue at least five (5) working days in advance of any scheduled maintenance, planned outages, or Service configuration changes that may interfere with device monitoring. Customer must notify LevelBlue immediately of any unscheduled activities that may interfere with device monitoring.
- Provide a security policy consisting of a list of desired Internet Protocol (IP)

protocols to be implemented, including source addresses, destination addresses, ports, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and a description of the protocols to be implemented.

- Provide traffic estimates to LevelBlue during the initial implementation of the Service and any time incremental bandwidth upgrades of over 1Mbps anticipated at a particular Customer Site.
- Provide the necessary network information requested by LevelBlue in order to allow LevelBlue to provision Security device management access into the LevelBlue SNOC.
- Identify a suitable test location during enablement and implementation to properly test desired Security Policies prior to opening all Sites on the MSS.
- Utilize internal Hosts and Servers that are properly maintained and kept up to date by the Customer. Servers, LAN devices, operating systems and other architecture components of a Customer's infrastructure need to be properly maintained and kept up to date by loading the most recent software upgrades and the latest available security patches. It is also the Customer's responsibility to make every reasonable effort to keep those platforms that connect to LevelBlue security devices free from infection from potential worms, Trojans, viruses, or similar security threats. LevelBlue is not responsible for patching or removing security threats on Customer maintained equipment, including all Host and Server equipment connected to LevelBlue-managed security devices.
- Provide and maintain a dedicated Plain Old Telephone Service ("POTS") line for the Term of the Services. The POTS line serves as a back-up access mechanism for connectivity between the SNOC and the LevelBlue CPE. It is through this link that LevelBlue will manage power down, or make changes to the LevelBlue CPE and operating parameters, as necessary. The installation and cost of this link is Customer's responsibility, and LevelBlue will work with Customer to coordinate installation based on availability of all MSS and Customer-required components. Customer agrees to ensure (i) that the POTS line is not disconnected and (ii) that the POTS line is not used for any other purpose, or (iii) not modified or changed in any way.
- Ensure that all Customer systems and networks (including but not limited to those which are outsourced), that connect with those belonging to MSS, implement appropriate security controls which are designed to prevent loss, disclosure, unauthorized access or service disruption. The Customer must also ensure LevelBlue will have unrestricted access to LevelBlue's assets, either via remote access or physical access as appropriate, for the proper operation of the Service.

Customer must also restrict access to and use of these systems and assets only by authorized Customer personnel. The use of the LevelBlue network and its facilities is intended for use by the Customer only, and not for those who may be interconnected with the Customer's systems and network.

- Immediately notify LevelBlue if a Customer suspects a security breach within the Customer's network.
- Administer individual IP addresses on a Customer's Local Area Network ("LAN").
- Define and maintain the Customer's own security policy and internal security response procedures. In the event there is an incident generated either from the Internet or within the Customer's enterprise, it is the Customer's responsibility to have appropriate mitigation contacts, processes, and procedures in place. LevelBlue will work with the Customer's designated security contacts according to LevelBlue procedures and notify the Customer of incidents identified by MSS. LevelBlue will make Customer-requested Security changes identified by the Customer.
- Properly package, ship and return all LevelBlue CPE upon termination or expiration of this Agreement. Failure to do so may result in additional Charges.

SD-2.8.8. Service Availability

Section Effective Date: 24-May-2016

LevelBlue utilizes scheduled maintenance windows to upgrade LevelBlue CPE, software, and facilities which may add capacity, new features, resiliency and which may provide fixes to known problems. Scheduled maintenance times are:

Scheduled Maintenance Table	
Region	**Times**
United States	Every Sunday – 3:15 a.m. until 4:45 a.m. Eastern Standard Time and Every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Note: If the 3rd Sunday of the month falls on a holiday or other special day, LevelBlue may reschedule the monthly maintenance window.	

SD–2.8.9. Support and Management

SD–2.8.9.1. Initial Consultation for a Customer

Section Effective Date: 04-Oct-2014

Review of Customer's inbound and outbound traffic-related security policies.

Review of security policy to allow LevelBlue to understand the data needs of the Customer, and to recommend policy changes to better align with Customer's desired functionality at that Site.

Review of a Customer's network topology or architecture, the physical arrangement of devices, circuits, sub-networks, and other components to determine general access requirements and discuss use within the Customer's architecture.

Installation Completion is defined as once a host or other device on a Site has been Pinged, a Customer's end-to-end connections have been verified, and LevelBlue has implemented the initial deployment of the MSS (initial security policy deployment).

SD–2.8.9.2. Network Monitoring and Management

Section Effective Date: 04-Oct-2014

LevelBlue's Security Network Operations Center ("LevelBlue SNOC") provides centralized 7x24 management and monitoring of the MSS and owns and manages all required components.

The LevelBlue SNOC provides monitoring of the hardware and software and diagnose/investigate problems for alerted malfunctions. Software maintenance is performed via patches and LevelBlue- approved software updates.

LevelBlue may perform extensive maintenance up to four (4) times per year and may also schedule planned maintenance. LevelBlue will use reasonable efforts to give Customer at least thirty (30) days prior notice (via email or other electronic means) of such scheduled or extended maintenance schedules. LevelBlue reserves the right to perform maintenance at any time in order to properly maintain the Service or LevelBlue's network. MSS is not designed to operate during scheduled maintenance (such as upgrade to Customer equipment, software, and capacity upgrades or the addition of new features).

LevelBlue will perform maintenance and updates of MSS system configurations in accordance with Customer-selected components. LevelBlue will make configuration changes, as directed by the Customer Site security liaison

LevelBlue will provide assistance to the Customer Site security liaison in planning and executing any MSS configuration changes when a critical or urgent security incident occurs.

LevelBlue will communicate with Customer's technical contact(s) for installations, moves, adds, or changes.

SD-2.8.9.3. Installation

Section Effective Date: 04-Oct-2014

Provide ordering, provisioning, configuration, and associated testing of the MSS components.

Configuration of LevelBlue's MSS infrastructure located at the Customer Site.

Configuration of LevelBlue's MSS infrastructure located in the LevelBlue SNOC. Registration of Customer information and security configuration in LevelBlue's databases in support of the MSS Service.

SD-2.8.9.4. Special Requests

Section Effective Date: 04-Oct-2014

For special requests, LevelBlue will invoice Customer an agreed upon engineering or enablement fee. These fees will be defined in a separate Change Control Process for the specific Customer request.

SD–2.8.9.5. Help Desk Support

Section Effective Date: 04-Oct-2014

All issues, questions or requests for assistance related to MSS are made to the designated LevelBlue Help Desk on a 7x24 basis by Customer-designated points of contact.

As part of the diagnosis, LevelBlue will dispatch an on-site technician to mitigate failures in device components at the Customer Site. Where possible, malfunctions will be mitigated remotely by SNOC technicians.

A “Trouble Ticket”, defined as the individual incident report LevelBlue opens for each outage or other issue with the MSS, will be opened for each incident. The Trouble Ticket begins when an LevelBlue SNOC has acknowledged and validated an LevelBlue problem, and when an LevelBlue generated ticket is opened. A Trouble Ticket resolution is defined when the incident is resolved to the satisfaction of both the Customer and LevelBlue and the Trouble Ticket is closed.

The centralized Customer Help Center provides 7x24 problem assistance.

SD–2.8.9.6. Problem Severity Code Definitions

Section Effective Date: 01-Oct-2014

LevelBlue will determine the severity of a Trouble Ticket when it is created or proactively identifies the cause of the incident. This will occur either when a Customer call is received or when the monitoring center identifies an incident. The following descriptions are provided as guidance to assist the Customer with appropriately understanding the priority and severity of an incident:

Severity	Description
1	Severity 1 is defined as the highest level of severity. A Trouble Ticket, as defined above, will be generated by LevelBlue in the event that LevelBlue detects a problem with the performance of the MSS. The types of alarms which will generate Severity 1 incident may include a Service Component interface(s) unavailable, failures of LevelBlue CPE or inability of a Customer sanctioned IP protocol from working through the equipment.
2	Severity 2 is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects an attack against the LevelBlue CPE. The types of alarms which will generate Severity 2 incidents are: a) unexplained root logins or access attempts to the equipment, b) unexplained Server file transfers or c) failed or interrupted component processes.
3	Severity 3 is defined as Trouble Tickets generated by LevelBlue in the event that LevelBlue detects certain system health problems with the LevelBlue CPE. The types of incidents which will generate Severity 3 alerts are: a) backup problems, such as backup failures or missing backup files, or b) an audit which reveals missing files; or c) Trouble Tickets generated when LevelBlue has specific and accurate information about specific Customer events.
4	Severity 4 is defined as Moves, Adds and Changes, and Deletes (MACDs). Severity 4 tickets are also generated when LevelBlue needs additional specific information about a Customer trouble.
5	Severity 5 is defined as changes associated with out-of-band testing.

SD–2.8.9.7. Problem Reporting

Section Effective Date: 04-Oct-2014

Incidents may be reported by telephone or electronically, where available and where LevelBlue specifies. The electronic support system is available 24 hours a day, 7 days a week, excluding the periods for maintenance.

SD–2.8.9.8. Managed Security Services Change Management

Section Effective Date: 28-Nov-2018

When using the Service, including the use of the Self Service Tool, Customer designs and sets all filtering and interception policies (Security Policies). LevelBlue undertakes only the implementation of the Security Policies as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings.

SD–2.8.9.8.1. LevelBlue Provided

Section Effective Date: 28-Nov-2018

If changes to Customer's security policy are necessary at a given Customer Site, LevelBlue will manage implementation of any resulting changes to the MSS platform deemed necessary by LevelBlue; these required changes may result in a one-time implementation charge for affected LevelBlue MSS components.

- Customers can request a change in configuration, optional features and/or functional support of installed MSS components. Changes are subject to LevelBlue approval and additional charges may apply.
- Scheduled software and hardware upgrades may result in an interruption of connectivity for a period of time depending on the complexity of the change.
- Charges for Customer requested changes will be handled via the Change Control Process, as outlined in section 5.1. Charges will be invoiced upon installation or cancellation of an order.
- Customers may request up to six (6) change requests per month, per device. Additional changes will incur an additional charge and will be handled via the Change Control Process.
- MFS-PB provides Support for up to ten (10) total authorized Customer contacts

- Six (6) MACD service requests per month per managed device are allowed

SD–2.8.9.8.2. Self Service Tool

Section Effective Date: 28-Nov-2018

As part of the Premises-Based Firewall Service, Customers can request or make policy changes on their security device via the LevelBlue Policy Self Service Tool ("Self Service Tool") within the Threat Manager Portal. The Self-Service Tool includes a policy automation capability. This capability allows for some MACD requests to automatically configure Customer's device(s) without manual intervention by an LevelBlue security engineer.

LevelBlue provides customers:

- Access to the Self-Service Tool based on the roles configured for each user ID.
- Information on how to navigate and use the Self-Service Tool.
- Support for the use of the tool as well as Manual implementation in the event the automation function of the Self-Service Tool becomes unavailable.

Customer provides:

- LevelBlue with the user ID of individuals with their pre-assigned access privilege.
- Customer owned Security Policies that will be configured for their respective sites and devices.

SD–2.8.9.9. Managed Security Services General Security

Section Effective Date: 01-Oct-2014

IP communication is facilitated by the use of authorized IP address pairs. These IP address pairs may be used to provide a level of authorization or security to allow only authorized pairs of IP addresses to communicate. IP address relationships for LAN communication that the Customer authorizes must be registered with LevelBlue Global Network Services.

SD-2.8.10. Service Activation Date

Section Effective Date: 23-May-2016

LevelBlue provides Service Activation for the Premises-based Firewall Service, Premises-based Firewall, Managed Intrusion Detection and Prevention Service, Host-based Intrusion Detection and Prevention Service, and the LevelBlue Proxy Service. Service Activation consists of the following elements:

- Provisioning LevelBlue owned equipment at the designated customer-premise location used to enable the managed security service capability (firewall, IPS, Proxy). Activating Customer in all of the required LevelBlue management systems to provide inventory control, monitoring, and management of the solution as well as any customer experience interfaces such as BusinessDirect.

The Service Activation will occur when LevelBlue has determined that the above steps are complete. Billing will begin upon Service Activation. Absent any delay due to LevelBlue, Service Activation will begin no later than thirty (30) days after equipment has arrived on Customer's site.

SD-2.8.11. Ownership

Section Effective Date: 23-May-2016

All rights, title, and interest in and to the Service, any Hardware or Software associated with the Service are and shall remain the exclusive property of LevelBlue.

SD-2.9. Education Security Bundle (ESB) — AT&T Dedicated Internet (ADI) with Premises Based Firewall (PBFW) bundle for E-Rate (Limited to E-Rate eligible Customers only)

SD-2.9.1. Product Summary

Section Effective Date: 10-Mar-2017

Education Security Bundle is an Internet security solution that combines LevelBlue Premises-Based Firewall and AT&T Dedicated Internet for E-rate customers. Education Security Bundle meets E-rate Category 1 funding requirements for an integrated Internet and firewall security service.

1. AT&T Dedicated Internet (ADI) provides a dedicated (not shared with other

schools or organizations), symmetrical (same upload and download bandwidth) Internet connection. AT&T Dedicated Internet bandwidth options available with Education Security Bundle range from 50 Mbps to 10 Gbps. Local access is provided via fiber-based Ethernet.

2. Premises Based Firewall Service—integrates with ADI to help protect against malware and attacks. Available firewalls support various Internet speeds. The service includes security reporting, stateful inspection, DMZ and Extranet support, and Unified Threat Management (UTM) options such as intrusion prevention and web filtering.

SD-2.9.2. Service Availability

Section Effective Date: 10-Mar-2017

ESB is available for purchase pursuant to a Service Agreement and Pricing Schedule. The rates, terms, and conditions applicable to this Service are not customizable. The ESB offer combines the ADI and PBFW in specific combinations, and only the combinations, as defined in the Pricing Schedule.

ESB is available for purchase pursuant to a Service Agreement and Pricing Schedule. The rates, terms, and conditions applicable to this Service are not customizable. The ESB offer combines the ADI and PBFW in specific combinations, and only the combinations, as defined in the Pricing Schedule.

SD-2.9.3. Service Limitations

Section Effective Date: 10-Mar-2017

- ESB is available only in the Mainland US (Not available in Alaska, Hawaii, Puerto Rico, US Virgin Islands or other territories) and is not available for resale.
- Limited to Service availability for: areas in the following states where an LevelBlue affiliate is the ILEC and is able to provide ILEC facilities to the customer site: Alabama, Arkansas, California, Florida, Georgia, Illinois, Indiana, Kansas, Kentucky, Louisiana, Michigan, Mississippi, Missouri, Nevada, North Carolina, Ohio, Oklahoma, South Carolina, Texas, Tennessee and Wisconsin.

SD-2.9.4. Service Components

Section Effective Date: 10-Mar-2017

- AT&T Dedicated Internet service
  - Available speeds ranging from 50 Mbps to 10 Gbps. Speeds are as set forth in the Pricing Schedule.
- LevelBlue Premises Based Firewall
  - The PBFW offer included in the ESB offer consists of the components set forth in the Pricing Schedule.

SD-2.9.5. Additional Applicable Service Guides

Section Effective Date: 10-Mar-2017

The following Services and Services Components are described in the additional Service Guide(s) stated below, incorporated by reference, and found in the LevelBlue Business Service Guide "Service Guide Library". Except as noted above, all terms and conditions applicable to these Services and Services Components apply.

AT&T Dedicated Internet Service - http://serviceguidenew.att.com/sg_flashPlayerPage/MIS

LevelBlue Bandwidth Service Guide - http://serviceguidenew.att.com/sg_flashPlayerPage/BWS

SD-3. Managed Intrusion Detection/Intrusion Prevention Service (MIDS/MIPS)

SD-3.1. MIDS and MIPS Overview

Section Effective Date: 01-Oct-2014

MIDS/MIPS" is a fully managed, attack recognition and response capability for network security that can be configured in either Promiscuous mode or In-Line modes of operation. The Promiscuous (IDS) mode provides an unobtrusive "sniffing" of traffic, where traffic is presented to a sensor for analysis. With the In-Line (IPS) mode of operation, traffic passes though the sensor and is inspected before it is allowed to pass on. Both modes support the dynamic responses of "shunning" (blocking an attacking IP address in a firewall or router) or "resetting" (sending a TCP reset to terminate the TCP session). Only the In-Line mode supports the "dropping" action (dropping offending packets or traffic).

- MIDS/MIPS are monitored 24 hours x 7 days a week. Intrusion detection sensing

sensors are placed at specific locations in the Customer Internet access, whether on a Customer Site or at a LevelBlue Internet Data Center. The intrusion detection sensing sensors monitor data packet header and payload information in an effort to detect possible malicious activity. If possible malicious activity is detected by LevelBlue and an alarm is generated, the LevelBlue SNOC responds based on the Customer signature policy.

- Each intrusion detection sensor is configured by LevelBlue, based on the Customer determined signature policy, with changes to the standard alarm and severity settings determined by the Customer. LevelBlue further implements the Customer signature policy by setting alarms to correlate with certain levels of malicious activity and by setting actions in response to any alarms. At all times, Customer is responsible for decisions relating to its sensor placement and signature profile. LevelBlue will establish procedures between the LevelBlue SNOC, and the Customer identified Security Contact(s) to request configuration changes to the Customer security policy.
- Prior to provisioning of MIDS/MIPS, LevelBlue will conduct a technical assurance review to validate that the proposed MIDS/MIPS implementation is technically feasible and supportable under the standard definition of the MIDS/MIPS.

SD-3.2. Features of MIDS and MIPS

Section Effective Date: 17-Nov-2025

- Configure MIDS/MIPS in Promiscuous (IDS) mode. LevelBlue can re-configure MIDS/MIPS in an In-Line mode upon Customer request provided it is supportable based on the desired Customer configuration.
- Apply default IDS Signature policy on any managed MIDS/MIPS devices
- Provide updated IDS Signature database
- Provide IDS reporting via the LevelBlue Portal
- Provide 24x7 Investigative Phone Support
- Notify Customer of Alerts: phone call to Customer Point of Contact (CPOC) for “High Severity” alerts and e-mail to Customer for “Medium Severity” alerts
- Provide profiling (enhanced tuning and data traffic analysis) to give Customer a baseline of its network or alarm activity for individual devices on its network
- Perform sensor tuning based on Customer environment
- Deploy custom signatures in consultation with Customer following approval of such signatures by LevelBlue. Customer will receive 20 concurrent custom

signatures.
- Perform Root Cause Analysis for High Severity Alerts

SD–3.3. Standard Components

Section Effective Date: 17-Nov-2025

- 24x7 security event monitoring and equipment management
- Sensor placement assistance within a LevelBlue Internet Data Center or Customer Premises
- In-band correlation of sensor data in the Customer network
- Incident response based on signature policies and traffic profiles of Customer sensors
- Periodic updates to Customer sensor profiles to help reduce false positive alerts or alarm activity not related to cyber intrusions
- On-line on-demand reports
- Customized incident report for each High Severity alert generated
- Access to Tier III technical analysts in connection with High Severity alerts

SD–3.4. Optional Service Capabilities

Section Effective Date: 21-Nov-2017

MIDS/MIPS is offered with the following additional Service Capabilities at an additional fee:

- Enhanced Threat Segments (“ETS”)
- Each IDS offer includes one monitored segment. Additional segments may be monitored by the inclusion of the ETS option, however, LevelBlue will assess a per segment Charge.
- LevelBlue Host Intrusion Detection/Prevention Services (“HIDPS”)
- HIDPS is a managed, attack recognition and response solution that uses host protection technologies. These host protection technologies are software application agent options available to Customer on a bundled or standalone basis and installed directly on Customer servers. HIDPS is designed to monitor for suspicious activity through system log files, application, and kernel calls, and observed network resource behavior and changes to critical system files. Depending on Customer requirements and the number of agents deployed, additional hardware may be deployed to segment Customers and optimize traffic

flow back to the management center.

SD–3.4.1. HIDSPS Options

Section Effective Date: 21-Nov-2017

HIDPS is comprised of one or more of the following software application

options. Host Intrusion Prevention Services (HIPS):

- The HIPS option is designed to combine behavioral rules and signatures to analyze non-encrypted data streams, attempt to block attacks and reduce the urgency of patches for new threats. The HIPS option utilizes sensor software that is placed behind a screening device.

Application Control:

- The Application Control option helps protect the Customer system from unknown security threats by controlling the software execution on the system. Application Control software is programmed to block unknown and unauthorized applications and code on servers and fixed-function devices. Application Control uses a centrally managed "whitelisting" solution which is a list of known software identified by the Customer.

Change Control (with File Integrity Monitor):

- The Change Control option allows Customer to monitor and prevent unauthorized changes to the file system, registry, and user accounts. Customer can view details of who made changes, which files were changed, what changes were made to the files, and when and how the changes were made. Additionally, the Change Control option allows Customer to write protect certain files and registry keys to help guard against unauthorized tampering.
- Change Control option also provides File Integrity Monitoring (FIM). FIM provides near real- time information to Customer about specific changes to the Customer file system, registry and user accounts, including the user and program used to make the change.

Availability of HIDPS Options:

Below are the available options based on the operating systems and hardware configuration

Note that only one selection from below can be supported on a given server:

- Windows and Unix Operating Systems
- HIPS Standalone (IPS Engine Only)
- Application Control Standalone
- Change Control Standalone
- Application Control and Change Control Bundle

SD–3.5. MIDS/MIPS Specific Customer Responsibilities

Section Effective Date: 01-Oct-2014

In addition to the Premises-Based Firewall Customer Responsibilities set forth in this Service Guide, the following shall apply:

- Installing and maintaining the Customer LAN environment.
- Identifying the placement of the intrusion detection sensor within its network. Customer decisions on sensor placement may impact the ability of the sensor to detect potential traffic threats and may impact the ability of certain applications to perform properly.
- Addressing any Service impacts as a result of Customer requested: dynamic “shunning” or dynamic test and “resetting.”
- Completing any necessary provisioning documentation in a timely manner as appropriate to the requirements of the LevelBlue MIDS/MIPS implementation schedule, including confirmation of sensor signature level settings or modification of LevelBlue-provided standard sensor signature level settings.
- Designating and updating, as necessary, primary, and secondary contacts to/for:
- Security, system administration and technical issues
- Service reporting
- Change management requests
- Access to the area on Customer Site where the LevelBlue CPE will be placed
- Escalation requests
- Receiving and consulting on service alarms to enable Customer initiated incident response.

- Immediately notifying LevelBlue if the Customer suspects a breach of security within the Customer network.
- Providing functionality testing assistance during implementation, problem and change management processes.
- Where an LevelBlue MIDS/MIPS intrusion detection sensor is connected to a Customer LAN, providing and fully managing the switch the sensor is connected to. Unavailability of switch can lead to unavailability of sensors.
- Verifying compatibility with the Services both initially and throughout the Term. Providing network and/or server, including Firewall, support to allow the flow of MIDS/MIPS traffic back to the LevelBlue MIDS/MIPS monitoring systems.
- Acquiring, installing, and maintaining a dedicated analog line (dial telephone connection per LevelBlue's specifications at the Customer Premises) and cabling to allow LevelBlue to connect the out-of-band access modem and device that LevelBlue provides for use with the Service and the CPE for purposes of remote management and problem resolution.
- Ensuring that the MIDS/MIPS has adequate capacity to support the communication link(s) to be monitored. Customer must inform LevelBlue of any bandwidth upgrades or increased traffic flows on the network segment to which the sensors are attached.
- Completing the LevelBlue MIDS/MIPS pre-deployment worksheet.
- Providing a network diagram and security policy to assist in the professional services activity of placing and configuring sensors, and base lining "normal" traffic to assist in establishing an IDS profile for each sensor.
- Providing a 7x24 security contact to receive and consult on alerts and to enable a Customer initiated incident response.
- Cooperating with LevelBlue in identifying severity levels for specific groups of attack signatures and escalation policies and procedures.
- Implementing an event response process to use when Customer receives security event notifications from the Service.
- If the Customer orders HIDPS, providing Public IP address(es), NAT IP address(es), or private IPs routable over the LevelBlue AVPN or EVPN network so that the software agents can connect via the Internet or VPN back to the LevelBlue GCSC operations.

- Installing any HIDPS

software.

Cross References

SD-2.8.7. Customer Responsibilities

SD-3.6. MIDS/MIPS Service Availability

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Service Availability applies to the MIDS/MIPS Service.

Cross References

SD-2.8.8. Service Availability

SD-3.7. Support and Management

SD-3.8. Initial Consultation for a Customer

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Initial Consultation for a Customer also applies to the MIDS/MIPS Service.

Cross References

SD-2.8.9.1. Initial Consultation for a Customer

SD-3.9. Installation

Section Effective Date: 01-Oct-2014

Premise Based Firewall Installation also applies to the MIDS/MIPS Service.

Cross References

SD-2.8.9.3. Installation

SD-3.10. Network Monitoring and Management

Section Effective Date: 01-Oct-2014

Premise Based Firewall Network Monitoring and Management also apply to the MIDS/MIPS Service.

Cross References

SD-2.8.9.2. Network Monitoring and Management

SD-3.11. Service Activation Date

Section Effective Date: 01-Oct-2014

Premise Based Firewall Service Activation Date also apply to the MIDS/MIPS Service. Cross References

SD-2.8.10. Service Activation Date

SD-3.12. Help Desk Support

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Help Desk Support also applies to the MIDS/MIPS Service.

Cross References

SD-2.8.9.5. Help Desk Support

SD-7.1.8.1. Service Activation Date

SD-3.13. Problem Severity Code Definitions

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Problem Severity Code Definitions also applies to the MIDS/MIPS Service.

Cross References

SD-2.8.9.6. Problem Severity Code Definitions

SD-3.14. Problem Reporting

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Problem Reporting also applies to the MIDS/MIPS Service.

Cross References

SD-2.8.9.7. Problem Reporting

SD–3.15. MIDS/MIPS Security Levels

Section Effective Date: 01-Oct-2014

High Severity Security Alerts

- High Severity security alerts constitute an alert or combinations of alerts that create a security threat or breach against critical aspects of the Customer business, including its service and systems. Examples of possible high severity alerts include but are not limited to denial of service attacks which consume enough bandwidth or CPU cycles to impact the Customer Service and/or the Customer network; or an identified attempt to gain root privilege on a Customer device through a monitored network or on a monitored device; or an attack that is escalating at such a rate that it is likely to eventually breach the system or render the MIDS/MIPS Service or the Customer network inoperable.

Medium Severity Security Alerts

- Medium Severity alerts, or combinations of alerts, are those that are less likely to place the Customer business or network in immediate risk of compromise, but may pose severe risks if not dealt with in a timely fashion. Examples of alerts at this level include but are not limited to attacks that are persistent and may degrade the system without impacting it significantly; or any attack that displays a strong understanding of the systems involved as this could indicate an attack using inside information.

Low Severity Alerts

- Low Severity alerts are alerts or combinations of alerts that typically do not pose severe risks but may indicate trends or patterns to suggest the potential for future impact.

SD-4. LevelBlue Proxy Services (APS) Overview

Section Effective Date: 09-Jan-2015

APS consists of a hardware proxy server and software proxy appliances to provide a scalable proxy platform architecture to help secure web communications and delivery of business applications. APS intermediates between the Internet and Customer for security and control of Web-based traffic and enforcement of policies. The standard capabilities of the APS include forward and reverse proxy servers. A forward proxy server will take requests from the Customer internal network and forwards them to the Internet. In forward proxies, the client server names the target server to which it seeks to connect. A list of supported protocols for forward proxy services will be provided to the Customer. A reverse proxy takes requests from the Internet and forwards them to servers in the Customer internal network. The outside requests will connect to the proxy and not the Customer internal network.

APS can be implemented in the Customer premises or an LevelBlue Internet Data Center. APS is available if Customer is also receiving any of the following LevelBlue Services:

- LevelBlue Premises-Based Firewall service
- LevelBlue Network Based Firewall service
- Certain LevelBlue Services that utilize Multi-Protocol Label Switching

  ("MPLS") technology.

APS has two configurations: Explicit or Transparent:

- Explicit proxy configuration requires users to configure their browsers, either manually or via a Proxy Auto-Configuration script, to specifically point to one or more proxy servers. This configuration provides automated failover in the event a proxy server becomes unavailable.
- Transparent proxy configuration does not require any user intervention. A Transparent proxy can be placed in-line of the traffic flow. Alternatively, traffic will need to be redirected by a layer-4 capable device using Web Cache Communication Protocol or Policy Based Routing.

User Authentication can be performed on the proxy appliance. APS offers support for either Active Directory or Lightweight Directory Access Protocol (LDAP) integration via the proxy appliances.

SD–4.1. Features of LevelBlue Proxy Services

Section Effective Date: 01-Oct-2014

APS provides the following features relating to Internet access (both inbound and outbound):

- Filters/controls Customer web browsing, logon to remote Hosts (Telnet) and complete file transfers using File Transfer Protocol's (FTP).
- Restricts access from the Internet into the Customer's corporate network.
- Provides a variety of access and utilization reports to help monitor Internet usage.
- Includes the installation of security on Customer premises that are linked directly into LevelBlue's SNOC. Customer Internet access takes place via LevelBlue Proxy Services, acting as protected gateways to the Internet. Once Internet-bound traffic reaches the Proxy Services, it is allowed access to or from the Internet based upon the Customer's specific Security Policy.
- Traffic is filtered by the Proxy Services and is routed from these gateways directly to and from the Internet. The Proxy Services is monitored and controlled by the SNOC.

SD–4.2. Standard Components of APS

Section Effective Date: 01-Oct-2014

APS provided the following features:

- 7x24 filtering of traffic through the Customer proxy running on hardware platforms.
- Standard outbound Customer security policy allowing identified Customer internal networks to access HTTP, HTTPS, and FTP sites.
- Customer-defined "rule elements" or "rules" that describe how the proxy processes traffic, which types of traffic should be accepted or denied, and which types of traffic should generate logs for subsequent analysis. Customer can specify and define the rules in its security policy.
- Virtual Router Redundancy Protocol ("VRRP") for assigning traffic across an HA Proxy Pair.
- A link back to the SNOC for monitoring access into the APS.
- Network Address Translation ("NAT") for internal IP aliases
- If User Authentication is requested by Customer, interface between APS and

Customer hosted and managed User Authentication service to authenticate User activity to the Internet. Customer will remain responsible for the provisioning, administering, support and/or troubleshooting of its User Authentication solution.

SD-4.3. APS Optional Components

Section Effective Date: 01-Oct-2014

ProxyAV option provides an anti-virus service that scans individual HTTP and FTP files for known viruses, malicious code, and other web-based threats. ProxyAV option consists of an Anti-Virus hardware Server and software agent for the specific anti-virus engine (i.e., Kaspersky, McAfee, Panda, Trend or Sophos).

The ProxyAV option includes:

- Antivirus scanning of HTTP and FTP attachments
- Automated detection of macro viruses in Web attachments
- Automated detection of harmful scripts in web pages
- Automatic virus pattern file updates
- Scanning of packets as they pass the Internet gateway
- Quarantine of files for cleaning or deletion.

ProxyAV option can scan files up to 2 GB in size and analyze up to 99 layers of compressed archives.

URL/Web Filtering Option supports enforcement of certain Customer defined Internet access policies by attempting to block undesirable web content while monitoring Internet activity.

URL/WF option is capable of categorizing billions of web pages in more than 50 languages into 85 useful categories (e.g., Sport, Shopping, Adult, etc). When deployed with APS, URL/WF Service can enforce and update corporate security policies across the network based on these categories and execute granular control over select popular web applications and operations.

The URL/Web Filtering (URL/WF) option includes:

- Default LevelBlue URL/WF policy applied on Enforcement node
- Latest URL/WF database from vendor maintained on Enforcement node

- Support for the use of LDAP integration for user/group specific filtering policy.

The SSL Proxy option is available to a Customer receiving the ProxyAV option. SSL Proxy option uses a hardware assisted encryption and decryption technology built into the proxy servers to create the capability of scanning encrypted traffic. It is designed to scan and stop malware, including viruses and spyware, from infiltrating network through encrypted tunnels. SSL Proxy option has policy settings to help optimize web traffic (e.g., scanning selected traffic instead of all traffic, or selected user groups instead of all users).

If Customer does not purchase the SSL Proxy option, APS will only perform rudimentary analysis based on the packet header information of encrypted traffic.

SD-4.4. Customer Responsibilities

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Customer Responsibilities also applies to APS.

Cross References

SD-2.8.7. Customer Responsibilities

SD-4.5. Service Availability

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Service Availability applies to APS.

Cross References

SD-2.8.8. Service Availability

SD-4.6. Support and Management

Section Effective Date: 01-Oct-2014

The Premise Based Firewall Support and Management apply to APS.

Cross References

SD-2.8.9. Support and Management

SD-4.7. Initial Consultation for a Customer

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Initial Consultation for a Customer also applies to the Proxy Service.

Cross References

SD-2.8.9.1. Initial Consultation for a Customer

SD-4.8. Installation

Section Effective Date: 01-Oct-2014

Premises-Based Firewall Installation also applies to the Proxy

Service. Cross References

SD-2.8.9.3. Installation

SD-4.9. Network Monitoring and Management

Section Effective Date: 01-Oct-2014

Premises-Based Firewall Network Monitoring and Management also apply to the Proxy Service.

Cross References

SD-2.8.9.2. Network Monitoring and Management

SD-4.10. Service Activation Date

Section Effective Date: 01-Oct-2014

Premises-Based Firewall Service Activation Date also applies to the Proxy Service. Cross References

SD-2.8.10. Service Activation Date

SD-4.11. Special Requests

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall special requests also apply to the Proxy Service.

Cross References

SD-2.8.9.4. Special Requests

SD-4.12. Help Desk Support

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Help Desk Support also applies to the Proxy Service.

Cross References

SD-2.8.9.5. Help Desk Support

SD-4.13. Problem Severity Code Definitions

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Problem Severity Code Definitions also applies to the Proxy Service.

Cross References

SD-2.8.9.6. Problem Severity Code Definitions

SD-4.14. Problem Reporting

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall Problem Reporting also applies to the Proxy Service.

Cross References

SD-2.8.9.7. Problem Reporting

SD-4.15. MSS Change Management

Section Effective Date: 01-Oct-2014

The Premises-Based Firewall change management also applies to the Proxy

Service. Cross References

SD-2.8.9.8.1. LevelBlue Provided

SD-5. Token Authentication Services SD-5.1. Features of the Service

Section Effective Date: 17-Nov-2011

LevelBlue offers two types of managed Token Authentication Service: Subscription and Dedicated.

Subscription Solution – Under the Subscription Solution, RSA Authentication Manager Servers are owned and managed by LevelBlue, physically located in LevelBlue IDCs, and accessed by the Customer and Users via the Internet. Under the Subscription Solution, LevelBlue maintains at least two replica servers for each primary Server for shared processing and redundancy. Each RSA Authentication Manger Server provided under this Subscription service authenticates multiple Customer applications.

Dedicated Solution – There are two choices available to Customers under LevelBlue's Dedicated solution – a) LevelBlue maintains and monitors an RSA Authentication Manager server dedicated to Customer's Users, or b) Customer may purchase RSA Authentication Manager Servers from LevelBlue. If a Customer elects to purchase the Dedicated Solution, Customer must also purchase at least one replica RSA Authentication Manager Server for each primary RSA Authentication Manager Server.

SD–5.2. Token Authentication Services Overview

Section Effective Date: 30-Apr-2022

LevelBlue's Token Authentication Service is a network access security technology that assists in allowing only authorized Users to the Customer's network with higher level of security than simple User ID and Password authentication.

- A User-created Personal Identification Number (PIN).
- A token code that is randomly generated by a physical device (token authenticator) in the User's possession. LevelBlue offers two types of managed Token Authentication Service: Subscription and Dedicated. Subscription Solution is described below, and Dedicated Solution is described under Optional Components.
- Subscription Solution – Under the Subscription Solution, RSA Authentication Manager Servers are owned and managed by LevelBlue, physically located in LevelBlue IDCs, and accessed by the Customer and Users via the Internet. Under the Subscription Solution, LevelBlue maintains at least two replica servers for each primary Server for shared processing and redundancy. Each RSA Authentication Manger Server provided under this Subscription service authenticates multiple Customer applications.

SD–5.2.1. Features of the Service

Section Effective Date: 10-Oct-2014

For both Subscription and Customized Solutions, LevelBlue will purchase the licenses and the Tokens on behalf of the Customer, along with an annual maintenance contract for the RSA Authentication Manager Server and bill Customers accordingly.

Customer's applications and network systems must be in compliance with the RSA Authentication Agent Software list provided at http://www.rsasecurity.com/node.asp?id=1174, and click on the operating system (Windows, UNIX, etc.) at the bottom of the page to get a list of supported platforms and system requirements for each agent available. LevelBlue will provide technical support to the Customer to facilitate proper configuration of devices accessed by RSA Authentication Agents for up to 10 RSA Authentication Agents. RSA Authentication Agents for optional platforms including open/VMS, Novell, OS390, CICS, and Lotus Domino may be provided at an additional charge and are not included in the initial RSA ACE Agent configuration included with the Service.

RSA Authentication Manager Servers are located in the LevelBlue IDC. IDC features include:

- Redundant and diverse network access capacity on an LevelBlue Local Services ring.
- 7x24 security including guards, closed-circuit monitors, alarmed doors, biometric scanner, etc. Building and environmental alarms are monitored locally by a 7x24 maintenance staff and also remotely by the LevelBlue S/NOC.
- Dual UPS in the IDC with diesel generator backup.
- IDC sites that have undergone extensive LevelBlue standards-based risk assessments to ensure they are at reduced risk of physical dangers.

As a part of this Service, LevelBlue also provides a standard monthly usage report with management information sent via email, containing elements such as:

- Number of allowable accesses
- Number of denied accesses
- New tokens assigned, and
- New PINs assigned

SD-5.2.2. Standard Components

Section Effective Date: 01-Oct-2014

Token Authentication Service is built upon components furnished to LevelBlue by RSA SecurID®. These components consist of:

SD-5.2.2.1. RSA Authentication Manager Server.

Section Effective Date: 17-Nov-2011

RSA Authentication Manager Server serves as the authentication engine for the Service. The RSA Authentication Manager Server enables two-factor authentication providing a central database for administration of user accounts. The features provided by the RSA Authentication Manager Server include setting and enforcing per user rules on access to private network systems, files, and applications. In addition, the RSA Authentication Manager Server provides the ability to define access, based on time of day, day of week, or by group or user -defined access; create logs of user access; and define and report alarm situations, such as repeated failed attempts to access a network port. In the event of primary RSA Authentication Manager Server failure, traffic is routed to the replica RSA Authentication Manager Server.

SD–5.2.2.2. RSA Authentication Agents

Section Effective Date: 17-Nov-2011

RSA Authentication Agents are the software intermediaries that enable authentication. RSA Authentication Agents are device-specific software agents, built into most leading network equipment, as well as Internet browsers and Web Server software systems.

SD–5.2.2.3. RSA SecurID® Authenticators

Section Effective Date: 17-Nov-2011

RSA SecurID® Authenticators when combined with a user's secret PIN, provides the pass code used in the two-factor authentication service. Two types of authenticators are used in the service. Hardware Authenticators or Key Fobs are end-user devices with a built-in chip that generates one-time token codes (every 60 seconds). Software Authenticators or Soft Tokens, provide symmetric key or "seed record" on the user's desktop, laptop, PDA, handheld, or mobile phone.

SD–5.2.3. Token Authentication Optional Components

Section Effective Date: 01-Oct-2014

The following optional components are available for LevelBlue's Token Authentication Service:

SD–5.2.3.1. Optional Component 2

Section Effective Date: 01-Oct-2014

Additional one-time assistance provided by the LevelBlue Professional Services team may be required at a separate charge for customized application support.

SD–5.2.3.2. Optional Component 1

Section Effective Date: 10-Oct-2014

Dedicated Solution – There are two choices available to Customers under LevelBlue's Dedication Solution.

- Evaluating the capacity, selecting, and configuring the RSA Authentication Manager Server to support the token Authentication Service.
- The engagement of LevelBlue's Professional Services team at an additional and separate charge for customized application support (as required).
- LevelBlue maintains and monitors an RSA Authentication Manager server dedicated to Customer's Users, or
- Customer may purchase RSA Authentication Manager Servers from LevelBlue. If a Customer elects to purchase the Dedicated Solution, Customer must also purchase at least one replica RSA Authentication Manager Server for each primary RSA Authentication Manager Server.
- Customer of the Dedicated Solution option may request customized reports from LevelBlue which are available on an individual case basis and as an additional one time and monthly cost.

SD-5.2.4. Customer Responsibilities

Section Effective Date: 01-Oct-2014

The following describes Customers responsibilities for each of the LevelBlue Token Authentication Service:

- An initial order for 25 tokens is required to purchase LevelBlue's Token Authentication Service.
- Customer is responsible for obtaining, installing, and maintaining suitable equipment and implementing and maintaining a protocol environment, computing platform, and operating system software as necessary for; and in a manner that permits the Customer to access the Service.
- Customer is responsible for obtaining, installing, and maintaining the RSA Client Software to enable use of Software Tokens on certified devices. Software is available on RSA Security Web site.
- Once a token is received by the Customer and activated by LevelBlue or the Customer, the monthly charges will be incurred until the User of the token is deleted from the RSA Authentication Manager Server and the token is revoked for use.
- In the event that a Customer loses or damages a token and requests a replacement, LevelBlue will provide the User with temporary access, and charge the Customer at the standard management fee for the token.

- Customers must order and activate the specified number of tokens contained in the contract for the Service. In addition, Customer may order additional tokens to have on hand for purposes such as token loss or damage, by paying the one-time token charge. Customer must work with Customer care to maintain adequate inventory for replacement and new token deployment requests. Customer must also coordinate with Customer care to approve procurement of replace inventory for expiring tokens. Customer may not return any such tokens for credit. Customer will be charged the monthly token management fee for each such token as of the date when LevelBlue or Customer activates a token. Customer shall have the right to terminate any individual User token ordered under its Attachment/Pricing Schedule at any time upon (30) days written notice to LevelBlue, as long as Customer maintains the minimum number of tokens specified in the Attachment/Pricing Schedule for the Service.
- Customer may remove Users from the RSA Authentication Manager Server and revoke any associated token(s) upon at least 30 days prior written or electronic notice to LevelBlue. In the event of an emergency, where potential security breeches may occur if such revocation requests are delayed, Customer's CPOC may request that LevelBlue immediately remove a User from the RSA Authentication Manager Server and revoke any associated token(s) via an email or a phone call to the appropriate LevelBlue Customer care facility.
- If a Customer wishes to delete a user from the RSA Authentication Manager Server or revoke a token, they must contact LevelBlue.
- Any bandwidth needed for back-end connectivity for the RSA Authentication Manager Server must be purchased and provided by the Customer.

SD–5.2.5. LevelBlue Token Authentication Country Availability

Section Effective Date: 10-Oct-2014

The Service is available in select countries in the following regions: a) Europe/Middle East/Africa ("EMEA") and b) United States as detailed in the table below.

Table of Regions	
Region	**Countries within a Region**
EMEA	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Lithuania, Luxembourg, Latvia, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom
United States	United States

SD–5.2.6. LevelBlue Token Authentication Service Availability

Section Effective Date: 01-Oct-2014

Service availability for Token Authentication Service is dependent upon the ability of the Customer's authentication requests to reach the RSA Authentication Manager Server. In the event that the request reaches the server but there are authentication problems, Customer must report the trouble to LevelBlue for further investigation. Severity levels for trouble tickets are determined as specified in the table below.

Trouble Ticket Severity Levels		
Severity Level	Description	Impact
Severity 1	Primary and replica RSA ACE/Servers are out of service	No authentication or help desk functions permitted
Severity 2	Primary down and the replica is operating	User will be able to authenticate. No help desk functions permitted
Severity 3	Primary operating replica is down	User will be able to authenticate. Help desk will be permitted to perform tasks

SD-5.2.7. Support and Management

SD-5.2.7.1. Initial Consultation for a Customer

Section Effective Date: 01-Oct-2014

The Customer Point of Contact (CPOC) will be contacted for training, setup, and provisioning.

SD-5.2.7.2. Assistance

Section Effective Date: 01-Oct-2014

LevelBlue provides Customer Help Desk support to assist users.

SD-5.2.7.3. Installation

Section Effective Date: 30-Sep-2014

All RSA Authentication Manager Server installations will be performed during normal business hours: Monday through Friday, 8:00 a.m. to 5:00 p.m. eastern time. Any work outside these hours will be provided at an additional cost and overtime/holiday rates may apply.

SD-5.2.7.4. Management

Section Effective Date: 17-Nov-2011

The managed token authentication technical operations team will provide the following 7 x24 support services:

- Monitoring Customers RSA Authentication Manager Server.
- Troubleshooting RSA Authentication Manager Server outage issues continuously until resolution.
- Identifying and applying Operating System software level patches that relate to security issues or known bugs affecting the operation of the RSA Authentication Manager Server or RSA Authentication Agent.
- Providing notification to CPOC of RSA Authentication Manager Server outages

within 30 minutes of an LevelBlue-validated RSA Authentication Manager Server outage issue and providing estimated repair time based on the severity level of the outage. Mailing of new tokens for delivery to sites within the US within 3 business days of receipt of an authorized request. Customer locations outside the US will be mailed within 4 business days.

- Termination request processing for CPOC's who may request the termination of any individual User token at any time upon (30) days written notice to LevelBlue, provided that Customer will maintain its minimum number of users as stated in the contract. In the event the Customer requests a termination for security reasons or revocation is otherwise urgently required, the CPOC will have the option to contact the helpdesk and LevelBlue will immediately revoke such user token upon ascertaining that CPOC meets identification requirements.
- Replacement of defective or damaged tokens, which will be mailed within 3 business days of receipt of notice (or 4 if the location is international).
- Token re-synchronization/PIN re-sets may be accomplished through a web-based interface or by calling LevelBlue and will be implemented upon validation of the User.

SD-5.2.7.5. Maintenance

Section Effective Date: 01-Oct-2014

Scheduled maintenance activities will be conducted with 48 hours advance notice to the Customer Point of Contact (CPOC) via email and during off-peak hours if possible. In the event that emergency unscheduled maintenance activities are required. LevelBlue will notify the CPOC via phone.

SD-5.2.7.6. Service Activation Date

Section Effective Date: 01-Oct-2014

Customer will be charged the monthly token management fee as of the date when LevelBlue or Customer activates the first set of tokens.

SD–5.2.7.7. Special Requests

Section Effective Date: 01-Oct-2014

The following describes LevelBlue's responsibilities for each of the LevelBlue Token Authentication Service:

- Lost or damaged tokens are replaced at the standard price for tokens contained in the Attachment/Pricing Schedule.
- Customer shall be charged the full installation rate in the event that Customer cancels or reschedules any installation without 3 days prior written notice.

SD–5.2.7.8. Help Desk Support

Section Effective Date: 01-Oct-2014

LevelBlue provides Customer Help Desk support to assist users with authentication questions/problems. The help desk service is centralized in the United States.

Token Authentication Tier 1 Support functions can be addressed directly by accessing a 7 x 24 x 365 secure website at https://www.e-access.att.com/token.

The Self-Help web site can be used to perform simple help desk functions such as resynchronization of tokens, password resets, replacement of lost or broken tokens and obtaining a temporary password.

SD–5.2.7.9. Problem Reporting

Section Effective Date: 01-Oct-2014

For help with issues that cannot be performed on the self-help web page, the user can contact the helpdesk by calling the number listed in the “Contact Us” link on the self-help web page

Callers dialing in to a help desk located outside their own country may incur a local access charge. As needed, LevelBlue help desk personnel may engage translation services via Language Line. In such case, translation services charges will be passed through to the Customer.

SD-6. LevelBlue Distributed Denial of Service (DDoS) Defense SD-6.1. Overview

Section Effective Date: 28-Feb-2017

The LevelBlue DDoS Service ("DDoS Service" or the "Service") can only be provided to ADI/ADI+/ADIG Customers and/or LevelBlue Internet Data Center ("IDC") Hosting customers with connectivity to the LevelBlue IP Backbone.

The DDoS Service includes DDoS detection and mitigation that takes place within LevelBlue's backbone and provides protection against volumetric attack traffic before reaching the Customer site. It consists of a network detection device, which examines samples of Customer traffic flow data from the LevelBlue network for each address identified by Customer. Upon detection, or Customer notification of a perceived DDoS Attack, LevelBlue can reroute traffic targeted at an attacked host through the LevelBlue IP Backbone to a shared Scrubbing device which then 'scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic. The DDoS Service is designed to then pass valid traffic to the Customer access router. LevelBlue will resume the normal routing of Customer traffic once LevelBlue determines the DDoS attack has subsided. The Customer will have access to reports on the attack and mitigation activity through a Customer-specific portal ("DDoS Defense Portal"). In addition, LevelBlue shall:

- During the first two (2) weeks following the Service Activation Date, examine samples of Customer traffic flow data and analyze patterns within such data in order to baseline Customer traffic patterns to assist in determining when a DDoS attack is occurring
- When LevelBlue believes that conditions so warrant; (a) issue Alert(s) to Customer about IP Threat(s) which shall direct Customer to the DDoS Defense Portal for further information; (b) provide information via the DDoS Service Portal to assist Customer in addressing and/or mitigating IP Threats
- Notify Customer via email within fifteen (15) minutes, and where warranted, by telephone within twenty (20) minutes, when LevelBlue believes a DDoS attack is occurring
- Provide Customer access to reports on specific attacks and mitigation activity through an LevelBlue specific website provided to Customer
- Make available to Customer the Traffic Anomaly Detection analysis and Traffic Anomaly Detection reports related to any DDoS Attacks on Customer during

the period in which DDoS Service is provided to Customer. All reports are LevelBlue Proprietary Information and are subject to the terms and provisions of the Agreement.

SD-6.1.1. Customer Responsibilities

Section Effective Date: 13-Sep-2013

Cooperate with LevelBlue in all aspects of the Service, including, but not limited to providing LevelBlue with the names(s) of a point of contact for the Service.

- Assure that only it or its designated Users will access the Service and that Customer and all Users will not share User IDs or other methods for accessing the Service with individuals who are not the designated Users of the Service. Customer further agrees to notify LevelBlue of the designated User of each User ID provided with the Service. Customer shall promptly notify LevelBlue of any changes to any of the designated Users assigned to the User ID, not disclose, copy, disseminate, redistribute, or publish any portion of the Service to any other party. Reproduction of the Service in any form or by any means is forbidden without LevelBlue's written permission, including, but not limited to: (a) information storage and retrieval systems; (b) recordings and re-transmittals over any network (including any local area network); (c) use in timesharing, service bureau, bulletin board or similar arrangement or public display; (d) posting any portion of the Service to any other online service (including bulletin boards or the Internet); or (e) sublicensing, leasing, selling, offering for sale or assigning the Service(s) to another entity or User
- Assure that its and User's use of the Service(s) will comply with written and electronic instructions for use of the DDoS Defense Portal
- Be solely responsible for determining the configuration of and how and where to use the DDoS Defense Portal views and reporting features. The portal views and reporting features of the Services are intended to provide Customer with information that is helpful in optimizing and otherwise managing its network and the Service purchased from LevelBlue
- Be the owner and controller of any data collected via these portal views and reporting features. LevelBlue shall be acting only as a data processor as to such information
- Be responsible either for (a) taking all relevant procedural steps to ensure that

viewing and using the portal views and reports is in compliance with applicable local laws and (b) ensuring that the portal views and reports are not used in countries where this is not permitted

- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to, providing LevelBlue information regarding any changes to the Customer network in order to assist LevelBlue in its analysis and examination of the Customer traffic flow date
- Provide LevelBlue with a list of Customer IP addresses connected to the LevelBlue IP Backbone that Customer wishes to have subject to the DDoS Service, and immediately notify LevelBlue of any additions or deletions to such list while Customer is receiving DDoS Service
- Provide LevelBlue with the names of three (3) Customer points of contact and related contact information
- Immediately notify LevelBlue of events that Customer becomes aware of that would cause significant traffic pattern changes in the Customer network that is being monitored under the DDoS Service; and
- Immediately notify LevelBlue if Customer believes it is under a DDoS attack and the Customer believes that LevelBlue failed to detect or notify Customer of such attack.

Customer acknowledges and understand that if Customer does not fulfill its obligations or provide the necessary information as provided herein, then the DDoS Service may be degraded or LevelBlue may not be able to provide the DDoS Service to Customer.

When using multi-ISP solution, Customer is responsible to:

- Ensure that the LevelBlue link is sized to support any additional traffic during the attack; and
- Withdraw the super block advertisement(s) from other ISPs.

SD-6.1.1.1. Additional Customer Responsibilities regarding DDOS Defense Service

Section Effective Date: 17-Nov-2011

Customer shall:

- provide LevelBlue with a list of Customer IP addresses connected to the LevelBlue IP Backbone that Customer wishes to have subject to the DDoS Option, and immediately notify LevelBlue of any additions or deletions to such list throughout the term of the service agreement
- provide LevelBlue with the names of three (3) Customer points of contact and related contact information
- immediately notify LevelBlue of events that Customer becomes aware of that would cause significant traffic pattern changes in Customer's network that is being monitored under the DDoS Defense Option
- immediately notify LevelBlue if Customer believes it is under a DDoS attack and the Customer believes that LevelBlue failed to detect or notify Customer of such attack

SD-6.2. Traffic Anomaly Detection

Section Effective Date: 01-Oct-2014

LevelBlue uses sampled traffic flow data from access routers within the LevelBlue network. This data is directed to the LevelBlue Anomaly Traffic Detection devices.

Traffic Anomaly Detection has two algorithms that run on a single detection portal. The first algorithm looks for "Misuse Anomalies" while the second algorithm looks for "Profiled Anomalies". Traffic Anomaly Detection, using both algorithms, is designed to detect anomalous traffic patterns that are considered malicious and to alert Customer that mitigation may be warranted.

SD-6.2.1. Methods of Detection

Section Effective Date: 17-Nov-2011

LevelBlue uses the NetFlow traffic from the access router within the LevelBlue network. The NetFlow traffic is directed to the LevelBlue Anomaly traffic detection device.

SD-6.3. Detection Capabilities and Exclusions

Section Effective Date: 01-Oct-2014

The DDoS Service is designed to detect and help protect against attacks that are volumetric in nature. For the purposes of this Service Guide, a volumetric attack is defined as an attack that sends high volumes of traffic designed to overutilize bandwidth and eventually deny access for legitimate users. Volumetric attacks include those attacks listed in the Volumetric Attack Types and Description table set forth below. Volumetric attacks do not include: (i) application layer attacks (those that primarily target applications); (ii) SSL attacks (those aimed at exploiting the CPU intensive nature of encrypting and decrypting packets); and (iii) "low and slow" attacks (those that consume a high number of connections and can exhaust server resources).

Volumetric Attack Types and Descriptions	
Attack Type	**Description**
Spoofed	Sending packets with a forged source address
Malformed	Sending packets with abnormal bits or flags set
Floods	Sending high rates of legitimately formed packets
Null	Sending packets with no content or illegitimate protocol
Fragmented	Sending packet fragments that will never be completed
Brute Force	Sending packets that exceed defined flow rates threshold

SD-6.4. DDoS Anomalies

Section Effective Date: 01-Oct-2014

Misuse Anomalies are traffic patterns that are of known DoS signatures including high rates of protocol fragments, ICMP, SYNs, RSTs and Nulls (No payload).

Profiled Anomalies are traffic patterns that have exceeded the learned baselines that have been generated by LevelBlue based on a sliding two-week interval of Customer traffic flow. Profiled thresholds are set at certain levels of Packets Per Second ("PPS") or Bits Per Second ("BPS") in excess of the pre-determined baseline.

Both Misuse Anomalies and Profiled Anomalies have three severity levels: LOW, MEDIUM, and HIGH. Low level anomalies are generated when traffic exceeds a minimum threshold. Medium level anomalies occur when the traffic exceeds a higher threshold value. A High-level anomaly occurs if the attack exceeds a higher threshold and is sustained for 300 seconds (5 minutes). An Alert is automatically generated in response to a High-level anomaly. Low and Medium level anomalies can be viewed via the DDoS Defense Portal. Anomaly notifications will be deleted after thirty (30) days if Low level, sixty (60) days if Medium level and one year if High level.

SD-6.5. Mitigation

Section Effective Date: 01-Oct-2014

Network Packet Scrubbing facilities utilize centralized DDoS mitigation devices to mitigate known malicious packets destined to the Customer network. A predefined BGP speaker will instruct a facility to re-route Customer traffic to one or more Scrubbing facilities. The BGP speaker will advertise the specific /32 address that is being attacked. This will reroute only that traffic targeted for the specific IP address to one or more of the LevelBlue Scrubbing facilities. After the Scrubbing facilities mitigate the malicious content, traffic determined to be valid will be forwarded back to the Customer through path that includes an LevelBlue managed virtual private network ("VPN"). Customer is not required to purchase VPN services from LevelBlue for mitigation to take place.

SD-6.6. Methods of Triggering

Section Effective Date: 13-Sep-2013

LevelBlue will activate the DDoS Service mitigation via BGP speaker within the LevelBlue network. During service enablement, Customer may choose between Automatic Mitigation and Manual Mitigation.

- Automatic Mitigation: When the LevelBlue detection device identifies a volumetric attack and provides an Alert to the S/NOC and the Customer, the work center will trigger the start of mitigation prior to notifying the Customer
- Manual Mitigation: When the LevelBlue detection device identifies a volumetric attack and provides an Alert, the S/NOC will consult with the Customer before any mitigation is activated.

In addition, in the event Customer identifies a volumetric attack, it can notify LevelBlue to request and activate mitigation.

SD-6.7. Annual Tests

Section Effective Date: 01-Oct-2014

Customer can request up to two (2) tests of the DDoS Service within one calendar year. A test must be coordinated with the LevelBlue Operations team and will consist of LevelBlue generating a volume of data traffic that will exceed Customer-defined thresholds as measured on network detection devices. A test is designed to simulate attack and to assess the systems for alerting Customer. Additionally, a test can confirm successful traffic mitigation as well as validate that valid traffic can be returned to the Customer site.

SD-6.8. Service Activation

Section Effective Date: 01-Oct-2014

LevelBlue provides Service Activation for the DDoS Service. Service Activation consists of the following elements:

- Provisioning LevelBlue equipment used for monitoring of Customer IP address blocks
- Identifying access routers on which Customer traffic is located
- Exporting Customer traffic flow data from access routers to a DDoS Defense Portal platform for analysis
- Activating Customer on the DDoS Defense Portal

The Service Activation will occur after the above steps are complete. Billing will begin upon Service Activation.

SD-6.9. DDoS Defense Portal

Section Effective Date: 01-Oct-2014

Reports of the DDoS Service are available to the Customer via the DDoS Defense Portal. Access to the DDoS Defense Portal is provided through the LevelBlue Security Center, which can be accessed through LevelBlue BusinessDirect®. The Customer is responsible

for maintaining LevelBlue BusinessDirect® Login IDs and appropriate access for individual users requiring access to the DDoS Defense Portal.

SD-6.10. Third Party ISP support

Section Effective Date: 01-Oct-2014

Service mitigation is only provided on the LevelBlue Common Backbone ("CBB"). Detection and mitigation can only be supported with traffic that terminates on an LevelBlue-provided Internet circuit.

In order for LevelBlue to provide mitigation for traffic on a third-party ISP network, the attack traffic will need to be rerouted to the LevelBlue CBB. Customer is responsible for understanding and coordinating the withdrawal of route advertisements from third party ISPs.

SD-6.11. Changes

Section Effective Date: 01-Oct-2014

If Customer is currently an LevelBlue Enterprise Hosting Customer and needs to make a change, either adding circuits or disconnecting circuits, Customer must advise its LevelBlue Sales Representative of such change so as not to negatively impact the DDoS Service that Customer receives. Service Level Agreements will not apply if Customer fails to notify LevelBlue of such change(s).

SD-6.12. DDoS Defense Welcome Kit

Section Effective Date: 01-Oct-2014

LevelBlue will provide Customer with an LevelBlue DDoS Defense Welcome Kit which includes an overview of the provisioning of the Service, FAQs, and other documentation.

SD-7. Grandfathered Offers

SD-7.1. Managed Intrusion Detection Service (MIDS)

SD-7.1.1. Overview

Section Effective Date: 17-Nov-2011

LevelBlue MIDS is a fully managed, attack recognition and response solution for network security. LevelBlue MIDS can be configured in either Promiscuous mode or In-Line modes of operation. The Promiscuous (IDS) mode provides an unobtrusive “sniffing” of traffic, where a copy of all interesting traffic is presented to a sensor for analysis. With the In-Line (IPS) mode of operation, traffic passes though the sensor and is inspected before it is allowed to pass on. Both modes support the dynamic responses of Shunning (blocking an attacking IP address in a firewall or router) or Reset (send a TCP reset to terminate the TCP session). Only the In-Line mode supports the Drop (drop offending packets or traffic) action.

MIDS is available at 3 levels of service:

- MIDS Level 1: An entry level, auto-response, template-based service. This feature is only available for deployment within the LevelBlue Internet Data Centers.\
- MIDS Level 2: Additional functionality including provision of initial technical consulting to customize the Customer’s Security Policy, their service architecture, and profiling the IDS sensors based on LevelBlue’s policies and procedures. This includes various types of automated responses.
- MIDS Level 3: A custom service tailored to meet Customer requirements and provide investigation support. Security Analysts monitor, report, and assist Customers with recommended mitigations.

LevelBlue MIDS will be monitored 24 hours x 7 days a week. Intrusion detection sensing components are placed at specific points in the Customer’s Internet access solution (depending upon the chosen level of service). This would either be at the Customers premises, or within their service components located at an Internet Data Center. For installations of intrusion detection sensors at a Customer premises location, LevelBlue is also able to place sensors within the Customer’s LAN. The intrusion detection sensing components monitor data packet header and payload information to detect possible malicious activity and the LevelBlue S/NOC responds to pre-defined events and alarms based on the Customer’s security posture. The Customer defines the signature policy by accepting the LevelBlue Design Documentation and Technical Provisioning Document prepared by LevelBlue for the Customer upon the basis of the Customer’s decisions.

The Service to be provided is subject to a technical assurance review by LevelBlue, following LevelBlue's current processes and procedures, to validate that the proposed MIDS implementation is technically feasible and workable under the standard definition of the Service. The Customer retains the responsibility to confirm their decisions for sensor placement and signature profile.

LevelBlue applies a signature policy that makes use of the intrusion detection sensor manufacturer-provided signature list and sets the alarm severity and resulting action. Each intrusion detection sensor will be configured by LevelBlue, based on the Customer determined signature policy, with changes to the standard alarm and severity settings determined by the Customer.

As part of the service implementation process, LevelBlue works with the Customer to determine the required settings.

Procedures will be put in place between the LevelBlue S/NOC and the Customer identified Security Contact(s) to request configuration changes to the policy and to act as a single contact point for Service issues.

Customers may request additional technical support, which is separately available at an additional cost, to provide support with any vulnerability assessment or risk evaluation that the Customer may require by signing the relevant agreement with LevelBlue.

SD-7.1.2. Features of MIDS Levels 1 – 3

Section Effective Date: 17-Nov-2011

The following table identifies the features and associated functionality by level for LevelBlue's MIDS Service offering.

Features of MIDS			
Feature/Functionality	**MIDS Level 1**	**MIDS Level 2**	**MIDS Level 3**
Network IDS/Host IDS (on Server)	NIDS and HIDS	NIDS only	NIDS and HIDS
7x24 Monitoring	Included	Included	Included
CPE Managed Option	Included	Included	Custom

Host Server Software IDS Option	Included	N/A	Included
Signature Updates Vendor Updates: Emergency	Included 3-5 business days 24 hours	Included 3-5 business days 24 hours	Included 3-5 business days, 24 hours
Incident notification	Email notification	Email notification for Medium and high, and additional telephone notification for High (4.6 contains further information)	Email for medium alerts within 15 minutes: High includes a telephone call (Section 4.6 contains further information)
Custom Reports	N/A	N/A	Optional

MIDS Sensor Configuration			
Feature/Functionality	**MIDS Level 1**	**MIDS Level 2**	**MIDS Level 3**
Initial Sensor Configuration	Standard Tuning	Standard Tuning	Custom Tuning
Continuous Sensor Tuning	Included	Included	Included
Custom Signatures	N/A	5	20

MIDS Sensor Location			
Feature/Functionality	**MIDS Level 1**	**MIDS Level 2**	**MIDS Level 3**
Location	IDCs	Any	Any

MIDS Security Analysis			
Feature/Functionality	**MIDS Level 1**	**MIDS Level 2**	**MIDS Level 3**
Alarm Analysis	Limited alarm set	Included	Included
Event Correlation & Analysis	N/A	Included	Included with additional real time

			analyst support
Root Cause Analysis for High Level Alerts	N/A	N/A	Included
Investigation Support	N/A	N/A	Included
Customer Notification based on SLO	Included	Included	Included
Attack Signature Recognition	Included	Included	Included
Dynamic Attack Blocking	N/A	Included	Included

MIDS CPE Software			
Feature/Functionality	**MIDS Level 1**	**MIDS Level 2**	**MIDS Level 3**
CPE Installation	Included	Included	Custom
CPE Maintenance	Included	Included	Custom
Software Installation	Included	Included	Custom
Software Maintenance	Included	Included	Custom
Problem Ticketing/Reporting	Included	Included	Included
Initial Configuration Support	Included	Included	Included
Configuration Maintenance	Included	Included	Included

SD–7.1.3. Network Access

Section Effective Date: 17-Nov-2011

LevelBlue MIDS supports the following access methods:

- MIDS Level 1: Internet access provided by LevelBlue at a US LevelBlue Internet Data Center
- MIDS Level 2:
- MIDS Level 3: LevelBlue Internet access specified in Level 1 and 2 or Internet access provided by an alternate Internet provider. In addition, any intrusion detection sensors at a Customer location or Internet data center must be Internet routable to allow management access to the S/NOC.

Refer to Section 4.8, Country Specific Provisions for local availability.

LevelBlue does not provide as part of this service any dissemination of generally available security information, including but not limited to, instant alerts or security advisories relating to threats and/or anomalies, such as, virus attacks, which may affect networks and their functioning.

MIDS sensor placement must be behind a screening device is preferred (i.e., Firewall, screening router, etc.).

SD-7.1.4. Service Limitations

Section Effective Date: 17-Nov-2011

The following limitations additionally apply to the Service provided:

The LevelBlue MIDS is not capable of analyzing encrypted data streams and would only be able to perform rudimentary analysis based on the packet header information in this scenario.

LevelBlue Level 1 and 2 are not designed (nor do they provide) the collection or substantiation or communication to the Customer of information that would qualify as evidence in support of any kind of recourse undertaken by the Customer following an intrusion. This includes, but is not limited to, an action against a person causing, either directly or indirectly, such an intrusion.

LevelBlue does not provide as part of this service any dissemination of generally available security information, including but not limited to, instant alerts or security advisories relating to threats and/or anomalies, such as, virus attacks, which may affect networks and their functioning.

MIDS Level 3 sensor placement must be behind a screening device (i.e., Firewall, screening router, etc.).

SD-7.1.5. Standard Components

LevelBlue provides the following Service features:

MIDS Level 1 Service includes:

- 7x24 security event monitoring and equipment management. Sensor implementation as determined by the Customer implementation guide, which must be in compliance with LevelBlue's standard guidelines for the service.
- LevelBlue assistance with tuning the signatures within the sensor as determined by the Customer, which must be in compliance with LevelBlue's standard guidelines for the service.
- Periodic refreshing of signatures within the sensors.
- Email incident notification for High and Medium Severity security alarms

(as further described in Section 4.6).

- Reports on a daily, weekly, or monthly basis MIDS

Level 2 Service includes:

- An LevelBlue developed and recommended IDS signature policy.
- Development of a Customer-determined sensor signature policy determined by the Customer in the Technical Provisioning Document, which must be in conformance with the vendor-provided signature set. Implementation of up to 5 unique IDS signatures per sensor and traffic direction to be defined by LevelBlue in response to anticipated or actual security threats.
- Standard "tuning" period, which will last for no longer than 14 days from the day that the sensor is initially activated.
- Ongoing management, maintenance and upgrade of all hardware and software components.
- LevelBlue Customer support available 24 hours a day, 7 days a week
- 7x24 security event monitoring and equipment management from the LevelBlue S/NOC following defined Security event response processes.
- Security event notification by automatically generated e-mail to the Customer security contact(s) for designated alarms and direct Customer contact by a pre-determined method for High Severity alarms.
- Security event correlation and analysis by the LevelBlue S/NOC including an initial response report for designated alarms.
- Customer determined, pre-defined, dynamic incident response (i.e., dynamic attack blocking, dynamic session reset), depending upon incident type and severity, for events as specified by the Customer as part of the Customer-specified signature policy for the manufacturer-supplied signature set or for the LevelBlue-defined unique signatures.
- Email notification for Medium and High severity alarms, and additional telephone notification for High, as determined by the Customer specific signature policy.
- On-going tuning of the unique signatures within each sensor. Any such requests must conform to LevelBlue's standard signature profile guidelines.
- Five Customer requested changes per sensor per month to the levels and actions

of manufacturer defined sensor signatures. These changes refer to any modifications to the existing configuration of the sensor including dynamic incident response and any signature tuning changes.

- Additional changes available as a charge option. Note: Any additional changes purchased by the Customer do not restart the initial service period.
- Regular vendor signature updates.
- All new IDS signatures from a sensor manufacturer will be implemented within 5 business days of release by the manufacturer(s) and after appropriate verification and testing process, and alarm level setting by the LevelBlue S/NOC. LevelBlue reserves the right to take longer than 5 days to implement the update or not to implement it at all.
- The LevelBlue verification process may result in the signature being implemented after the 5business day target or not being implemented.
- LevelBlue will make reasonable efforts to implement emergency updates by sensor manufacturers within 24 hours or earlier based on severity, testing, and verification by LevelBlue.
- Change request initiation via an LevelBlue provided contact point. Web enabled reporting on a daily, weekly, or monthly basis via an LevelBlue provided Web interface.

MIDS Level 3 Service includes:

- Provide 7x24 security event monitoring and equipment management.
- Sensor placement assistance within an LevelBlue Internet Data Center or a Customer location.
- Provide profiling (enhanced tuning and data traffic analysis) and professional services to give a baseline of the network or Host alarm activity, including analysis and verification by LevelBlue.
- Develop customized alert levels, through use of LevelBlue's proprietary tools and correlation database, so that alarms from individual sensors are correlated to alerts and categorized for response/reporting.
- Perform in-band correlation. In-band correlation refers to LevelBlue proprietary analysis of sensor data in a Customer's network, both individually and collectively.
- Provide incident response based on signature policies and traffic profiles of

Customer's sensors.

- LevelBlue periodically updates Customer sensor profiles to minimize false positive alerts or alarm activity not related to cyber intrusions.
- Provide root cause analysis where LevelBlue will determine the source, destination, and type of attack for alerts and provide Customer with specific information on each incident.
- Provide on-line reports on a daily, weekly, or monthly basis. A customized incident report is also provided for each High-Level alert.
- Provide technical support related to High Level alerts, where Customers will interface with (Tier III) technical analysts.
- Provide technology updates to support the updating of intrusion signature databases, used to trigger alarms for known attacks.
- Regular vendor signature updates:
- All new IDS signatures from a sensor manufacturer will be implemented within 5 business days of release by the manufacturer(s) and after appropriate verification and testing process of alarm level settings by the LevelBlue S/NOC. LevelBlue reserves the right to take longer than 5 business days to implement the update or not to implement it at all.
- The LevelBlue verification process may result in the signature being implemented after the 5-business day target or not being implemented.
- LevelBlue will make reasonable efforts to implement emergency updates by sensor manufacturers within 24 hours or earlier based on severity, testing, and verification by LevelBlue.
- Customer determined, pre-defined, dynamic incident response (i.e., dynamic attack blocking, dynamic session reset), depending upon incident type and severity, for events as specified by the Customer as part of the Customer-specified signature policy for the manufacturer-supplied signature set or for the LevelBlue-defined unique signatures
- Web enabled reports via a LevelBlue provided Web interface. Custom reporting is provided upon demand.

SD–7.1.6. Customer Responsibilities

Section Effective Date: 21-Mar-2012

The following describes Customers responsibilities for each of the available MIDS levels.

MIDS Level 1 and Level 2:

- Installing and maintaining the Customer LAN environment.
- Providing leased line, dedicated, network access at each Customer site.
- Identifying the placement of the intrusion detection sensor within its network. A Customer's decision relative to sensor placement may impact the ability of the sensor to detect potential traffic threats and may impact the ability of certain applications to perform properly.
- Any service impacts as a result of Customer requested dynamic shunning or dynamic test and reset.
- Providing the necessary information, including network diagram and Security Policy, for the Customer's network and Server environment to LevelBlue as part of the provisioning process and during the lifecycle phase of the Service.
- Completion of provisioning documentation in a timely manner as appropriate to the requirements of the LevelBlue MIDS implementation schedule, including confirmation of sensor signature level settings or modification of LevelBlue-provided standard sensor signature level settings.
- Providing LevelBlue or its designated agents' access to Customer premise for the purpose of installation and maintenance of the Service and its components as required.
- Designating primary and secondary contacts to/for:
- Security, system administration and technical issues.
- Service reporting
- Change management requests
- Receive and consult on service alarms and to enable Customer initiated incident response
- Work with LevelBlue on all matters related to this service.
- Ensuring that Customer security contact information provided to LevelBlue is up to

date and appropriate including timely notification of any changes.

- Immediate notification to LevelBlue if the Customer suspects a breach of security within the Customer's network.
- Notifying LevelBlue at least five working days in advance of any scheduled maintenance, planned outages, or Service configuration changes that may interfere with device monitoring. Customer must notify LevelBlue immediately of any unscheduled activities that may interfere with device monitoring. Designating a contact that has access to room and space where the equipment at the Customer premises will be held.
- Providing functionality testing assistance during implementation, problem and change management processes.
- Where an LevelBlue MIDS intrusion detection sensor is connected to a Customers LAN, provide and fully manage the switch the sensor is connected to.
- Customers must ensure compatibility with the Service both initially and throughout the service period. It is essential in this case to make sure the Customers switch will support the functions required for the MIDS.
- The LevelBlue management demarcation point is the MIDS Sensor "detection" interface.
- Sensor availability is fully impacted by the unavailability of the Customer- provided switch.
- Provide network and/or Server, including Firewall, support to allow the flow of MIDS traffic for management purposes.
- Acquiring, installing, and maintaining a dedicated analog line (dial telephone connection per LevelBlue's specifications at the Customer premise) and cabling to allow LevelBlue to connect the out-of-band access modem and device that LevelBlue provides for use with the Service and the CPE for purposes of remote management and problem resolution.
- Provide a better dedicated, secured, lockable, environmentally appropriate, and ventilated space that will accommodate the dimensions of the equipment.
- The impact of any action that is part of the Customers obligation for MIDS upon any other service provided to the Customer, by LevelBlue or a 3rd Party supplier.
- Ensuring that the LevelBlue MIDS does not conflict with any service provided by an

agreement between the Customer and a 3rd Party supplier, and the Customer is responsible for any impacts or conflicts that may occur including their satisfactory resolution at the Customers expense they prevent the provision of the LevelBlue MIDS; the Customer remains liable for the charges due to LevelBlue during such period.

- Ensuring that the LevelBlue MIDS supplied has adequate capacity to support the communication link(s) to be monitored. Customers must inform LevelBlue of any bandwidth upgrades or increased traffic flows on the network segment to which the sensors are attached.

MIDS Level 3

- Complete required LevelBlue MIDS Level 3 pre-deployment worksheet.
- Provide a network diagram and Security Policy to assist in the professional services activity of placing and configuring sensors, and base lining “normal” traffic to assist in establishing an IDS profile for each sensor.
- Provide a 7x24 security Customer contact to receive and consult on alerts and to enable a Customer initiated incident response.
- Immediately notify LevelBlue if a Customer suspects a security breach within the Customer’s network. Notifying LevelBlue at least five working days in advance of any scheduled maintenance, planned outages, or Service configuration changes that may interfere with device monitoring. Customer must notify LevelBlue immediately of any unscheduled activities that may interfere with device monitoring.
- Cooperate with LevelBlue in identifying severity levels for specific groups of attack signatures.
- Cooperate with LevelBlue in identifying escalation policies and procedures.
- Provide updated escalation contacts and reach numbers as they change.
- It is recommended that the Customer implement an event response process to use when Customer’s receive security event notifications from the Managed Intrusion Detection Service. Due to the diverse nature of security events, international regulations and Customer environments, the Customer is solely responsible to establish any such events response processes for their use.

SD-7.1.7. Service Availability

Section Effective Date: 17-Nov-2011

The LevelBlue MIDS is designed to be available 24 hours a day, 7 days a week, except for the following instances:

- During scheduled/unscheduled maintenance windows
- During systems upgrades/sensor tuning
- During connectivity or network outages
- Note that during any of these instances, alarm notification to the Customer may be delayed.

SD-7.1.8. Service Activation, Support and Management

SD-7.1.8.1. Service Activation Date

Section Effective Date: 17-Nov-2011

The scheduled Service Activation Date is agreed upon after receipt of a signed contract. Billing will begin on the Service Activation Date, which occurs at the end of a tuning period after successful verification tests are complete, including verification of the Customer determined signature Policy, which shall occur no later than 14 days after the initial activation of each sensor. However, if LevelBlue is unable to complete the installation of a sensor because of Customer actions, including the unavailability of Customer's final Security Policies or configurations, billing will commence on the original scheduled Service Activation Date.

SD-7.1.8.2. Support

Section Effective Date: 17-Nov-2011

LevelBlue will provide the following support as part of the LevelBlue MIDS as determined by the service level selected by the Customer:

- Delivery of the LevelBlue MIDS sensors.
- Provisioning of the Service Components, which may include some of the following: intrusion detection sensors, switches, out-of-band access and remote power equipment, router and cables depending on the configuration.

- Registration of Customer information and security configuration in LevelBlue's databases that is required by LevelBlue to deliver the Service.
- Project management and on-site installation of LevelBlue equipment.
- Implementation during local business hours at the local site (generally 9 am – 5 pm).
- Configuration of the Customer IDS according to the agreed signature parameters defined by the Customer.
- Ongoing management, maintenance and upgrade of all hardware and software components, provided by LevelBlue as part of the Service.
- 7x24Customer support.
- Proactive monitoring and emergency procedures
- 7x24 monitoring of sensor availability from the LevelBlue S/NOC of all LevelBlue supplied components.
- Problem management: logging, tracking and escalation of reported problems based on pre- determined severity levels set by Customer.
- Communication with the Customer designated security contact(s) on service-related issues including:
- Security, system administration and technical issues.
- Service reporting
- Change management requests
- Receive and consult on service alarms and to enable Customer initiated incident response
- Work with LevelBlue on all matters related to this service.
- Management and implementation of Customer-requested signature changes (as described in the table in Section 4.2.)
- Provision of defined Service reports and facilities via the LevelBlue web portal.

SD–7.1.8.3. MIDS Level 1 Event Response

Section Effective Date: 17-Nov-2011

- Fully automated logging and problem alerting processes.
- Automated notification to the designated Customer Security Contact(s) by the LevelBlue S/NOC for alarms.
  Event detection at the LevelBlue management center and automated notification of alerted event via E-Mail to the Customer security contact(s) within 15 minutes of the signature trigger on a sensor. This time interval is dependent upon LevelBlue's ability to communicate with the sensor.
- E-Mail delivery time is additionally dependent on the appropriate network transport and mail servers being available and is not a responsibility of LevelBlue as a part of this Service.

SD–7.1.8.4. MIDS Level 2 Event Response

Section Effective Date: 17-Nov-2011

- LevelBlue will provide management, service support and event response from the LevelBlue S/NOC including the following features:
- Fully automated logging and problem alerting processes using the LevelBlue Integrated Global Enterprise Management System (iGEMS), a sophisticated, end-to-end global network management platform that enables LevelBlue to monitor and manage the performance of clients' networks and associated applications in a proactive, predictive, and preventative manner.
- Logging of full data packet information may be performed, for a maximum of 15 minutes, after the trigger of a defined sensor signature. This feature is enabled and the data is logged by the LevelBlue S/NOC for problem determination, investigation and analysis purposes only. LevelBlue will only enable this feature for potential or ongoing security threats or violations.
- Direct notification to the designated Customer Security Contact(s) by the LevelBlue S/NOC for High-level alarms.
- In the event of virus/worm outbreaks/detection on the customer's network, the

S/NOC will notify the Customer with all appropriate details and inform the Customer that that no additional notifications will be made until the Customer advises us that the virus/worm has been cleared from their network or one month has elapsed since initial S/NOC notification.

- Attack mitigation on the LevelBlue managed router and/or Managed Firewall, if provided, dependent on either.
- S/NOC receiving the alarm, consulting the Customer Security Policy and evaluation of event, or
- S/NOC receiving notice from the Customer of the actions they would like the LevelBlue S/NOC to take.

SD-7.1.8.4.1. The following specific targets are applied to the event response process:

Section Effective Date: 17-Nov-2011

- Event detection at the LevelBlue management center and automated notification of alerted event via E-Mail to the Customer security contact(s) within 15 minutes of the signature trigger on a sensor. This time interval is dependent upon LevelBlue's ability to communicate with the sensor.
- E-Mail delivery time is additionally dependent on the appropriate network transport and mail servers being available and is not a responsibility of LevelBlue as a part of this Service.

SD-7.1.8.5. MIDS Level 3 Event Response

Section Effective Date: 17-Nov-2011

The following event response process will apply for MIDS Level 3:

- An automated correlation of intrusion events, adding LevelBlue proprietary analysis tools and trained security analysts to respond to alerts in accordance with a Customer's individual Security Policy.
- Technical support personnel will work with Customers in establishing the specific signatures and their associated severity level alerts and any service level objectives that may be available. This process will take place during the initial sensor tuning period to ensure that the alerts and severity levels are tailored to

meet the Customers requirements.

SD–7.1.8.6. Severity Alert Definitions

Section Effective Date: 17-Nov-2011

The following definitions clarify each of the MIDS severity levels:

SD–7.1.8.6.1. High Severity Security Alerts

Section Effective Date: 17-Nov-2011

High severity alerts constitute an alert or combination of alerts that define a security threat or breach against critical business/service/systems. Examples of possible high severity alerts are denial of service attacks which consume enough bandwidth or CPU cycles to impact the Customers service; or an identified attempt to gain root privilege on a Customer device through a monitored network or on a monitored device; or a non-severe attack that is escalating at such a rate that it is likely to eventually breach the system or render service inoperable.

SD–7.1.8.6.2. Medium Severity Security Alerts

Section Effective Date: 17-Nov-2011

Medium severity alerts, or combination of alerts, are those that do not place the business

/service/system in immediate risk of compromise but may pose severe risks if not dealt with in a timely fashion. Examples of alerts at this level are attacks that are persistent and may degrade the system without impacting it significantly; or any attack that displays a strong understanding of the systems involved as this could indicate an attack using inside information.

SD-7.1.8.6.3. Low Severity Alerts

Section Effective Date: 17-Nov-2011

These are alerts or combinations of alerts that do not pose severe risks but may indicate trends or patterns that might suggest future impact. Examples of alerts at this level are port scans originating from the Internet that may indicate reconnaissance for a future attack, or any unusual traffic patterns.

SD-7.1.8.7. Help Desk Support

Section Effective Date: 17-Nov-2011

All problems, questions or requests for assistance related to the MIDS should be made to the designated LevelBlue help desk support. Problems may be reported by telephone or electronically, where available as specified by LevelBlue. The time an incident starts is when a Customer speaks to the help desk, or when a Customer submits an electronic notification, or when an LevelBlue generated ticket is opened, as the case may be.

US Centralized Customer Help Centers provide 7x24 problem assistance.

SD-7.1.8.8. Service Reporting

SD-7.1.8.8.1. MIDS Level 1:

Section Effective Date: 17-Nov-2025

Reports are available and accessible via a web portal and categorized by event type and IP address.

SD-7.1.8.8.2. MIDS Level 2 and 3:

Section Effective Date: 17-Nov-2025

LevelBlue will provide reporting, which will be available via an LevelBlue managed services portal. The Customer will be provided with highly secure User IDs and passwords to enable access to the portal and are fully responsible for the use and management of these User IDs.

SD–7.1.8.8.3. MIDS Level 2:

Section Effective Date: 17-Nov-2025

MIDS Level Web enabled reports on a daily, weekly, or monthly basis via a LevelBlue provided Web interface.

SD–7.1.8.8.4. MIDS Level 3:

Section Effective Date: 17-Nov-2025

As part of the data gathering that takes place during enablement of the Service, LevelBlue will gather Customer contact details for the reporting system.

Reports are available on a daily, weekly, and monthly basis.

SD–7.1.9. Optional Components

Section Effective Date: 28-Feb-2017

The following table describes the optional features available as a part of this service, and the Levels that apply to each:

Optional Components		
Features	**Level**	**Description**
Expanded URL Filtering # of Concurrent Users 100, 500, 1000, 3000, 5000, Above (ICB)	1,2,3,4,5	Allows user to choose the additional feature option with an expanded number of URL Categories (80+) allowing for a more refined URL filtering policy. This feature provides customers with the ability to allow or block access to Internet web sites by category, black list and white list and source IP.
Application Filtering	1,2,3,4,5	Provides inline scanning of HTTP and FTP content for common virus, spyware, and malware threats and vulnerabilities. Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo, and AIM). Not available with Network Based Firewall on ADI. Reporting functionality is not available at this time.
Active IDS/IPS-Basic	1,2,3,4,5	Service includes IDS/IPS initial technical consultation and applies LevelBlue's best practices policy. Also includes IDS policy customization and addition of a limited set of custom IDS signatures to the profile as well as proactive investigational analysis for critical events and enablement of a limited set of automated IPS capabilities. Not available with Network Based Firewall on ADI.

Optional Components		
Features	**Level**	**Description**
Active IDS/IPS-Advanced	1,2,3,4,5	Provides a more customized service level and alert thresholds to meet more specific IDS requirements including a higher degree of profiling and tuning of IDS policy to strip out “noise” and provide notification on critical events. Additionally, LevelBlue Security Analyst provides live investigational analysis for all IDS events assisting with recommended mitigation actions and making firewall policy changes to eliminate a threat if warranted. Not available with Network Based Firewall on ADI.
Additional Networks	2,3,4,5	Based on customer definition/design, configure NBFW policies for each network segment needed, then joining that network and injecting default or host routes. Note that the chosen Service Level determines the number of rules, so the total of all rules under a solution needs to be within those bounds. A DMZ or other isolated MPLS network is considered to be another Network. Additional Networks are not available with NBFW on ADI.
Additional Public IPv4 Addresses (blocks of 4 or /30	2,3,4,5	If the customer needs more than the allocated number of IPv4 addresses for that Service Level, they can buy extra IP addresses. The benefit of this option is additional NAT functionality. The IP addresses can be bought as listed below: Multiple blocks of /30 IP addresses. Each /30 block gives 4 usable IP addresses. A single /30 IP address range must stay with each SDC (no individual IP addresses can be spread from a single /30 to multiple sites). Each /24 block gives 256 usable IP addresses. A single /24 IP address range cannot be broken into less than 32 IP addresses (i.e. a /27 subnet) for a single SDC. Addition Public IP Address are not available with NBFW on ADI.

Optional Components		
Features	**Level**	**Description**
Additional Site Egress	1,2	Allows outbound access from more than one SDC. For each additional SDC the pricing will be based on the bandwidth required for each connection (Secnet). Each extra SDC includes a /30 range of public IP addresses. Each /30 block gives 4 usable IP addresses. Additional Site Egress is not available with NBFW on ADI.
Additional Site Egress & Ingress	3,4,5	This option allows the customer to have inbound and/or outbound access through more than one SDC. They can select multiple SDCs. For each additional SDC there will be the following elements: A /30 range of public IP addresses, this includes the PAT (overload) address. Each /30 block gives 4 usable IP addresses. Two additional ePVCs for each extra SDC. Policy setup and support for each SDC. Additional Site Egress & Ingress is not available with NBFW on ADI.
Additional Firewall Rules (multiple blocks of 5)	2,3,4,5	Allows the user to choose this additional feature to purchase additional firewall rules if they go beyond their included number of rules for their Service Level.
Cross Connect	1,2,3,4,5	Provides connections between the NBFW instance in a Data Center location and the customer's cage in the same Internet Data Center. Cross Connect options supported are where the equipment in the cage is 1. managed by MSS Operations, 2. the equipment is managed by the customer, or 3. the equipment is managed by Managed Hosting Operations. Cross Connect is not available with NBFW on ADI.

Optional Components		
Features	**Level**	**Description**
Site Failover	2,3,4,5	This option allows the customer to have a single alternate SDC in the same geographical region to receive “failover traffic”. A 3rd ePVC is provisioned from the alternate site to the customer’s MPLS network. A duplicate security policy is maintained on the alternate SDC for a specified SecNet. If a customer has multiple SecNets, they must purchase Site Failover for a specific number of SecNets. Special requirements apply for Network Based Firewall Failover which have to be followed for proper operations and which would be considered during the design phase. Site Failover is not available with NBFW on ADI.
Advanced Logging	1,2,3,4,5	Deliver hourly syslog formatted log feeds to a customer hosted FTP server if requested.

SD–7.2. Managed Firewall Service – Network Based (MSS-NB)

Section Effective Date: 09-Jan-2015

The Managed Firewall Service – Network Based Service (MSS-NB) set forth in this Section are no longer available for purchase to new Customers as of October 1, 2014. Those Customers with previous MSS-NB may continue usage of such MSS-NB pursuant to the terms of their Pricing Schedule.

SD–7.2.1. Overview

Section Effective Date: 28-Feb-2017

LevelBlue MFS-Network Based firewall is designed to help enterprises implement and monitor Internet access for multiple sites. The Service will enable businesses to support and enforce sophisticated network Security Policies from one or more of the LevelBlue Internet Data Centers where the Network Based Security platform reside, also referred to as the Security Data Center (SDC). Customers are able to more efficiently implement a consistent Security Policy for multiple sites.

Designating configuration complexity, there are five levels available as a part of LevelBlue's MSS- Network Based service. These levels are:

Level 1: Outbound Only, Common Security Policy.

Level 2: Outbound Only, Custom Security Policy (up to 10 rules are included).

Level 3: Outbound/Inbound, Custom Security Policy (up to 30 rules included).

Level 4: Outbound/Inbound, Custom Security Policy, up to 50 rules included).

Level 5: Outbound/Inbound, Custom Security Policy, up to 99 rules included. As part of the Network Based Firewall on ADI transport ("NBFW on ADI"), only one outbound configuration is available – NBFW on ADI service type Outbound Only. There is a Custom Security Policy (up to 6 rules are included) in addition to the Common Security Policy.

For levels two through five, Customers are able to define their own Security Policies. LevelBlue completes the policy administration on the equipment. Levels 2 through 5 also feature optional content filtering and user authentication capabilities. Customers can obtain additional features, such as blocking access to specified web sites, and support for extranets via a monitored, private connection between the Customer and a business partner.

NBFW on ADI Customers are able to define their own Security Policies. URL Filtering and IDS logging only are part of the Service.

MSS-Network Based Firewall enforces traffic separation among Customers by enabling Virtual Local Area Network (VLAN) tagging. For Customers who wish to make use of the LevelBlue MFS- Network Based (MFS Firewall service, LevelBlue will establish a Private Virtual Circuit (PVC) from a Customer location to the service in order to filter the traffic coming in or going to the Internet. The type of PVC will vary based on the Customer's WAN architecture. Traffic separation is designed to occur without tunneling or encryption. This is enabled through a combination of Border Gateway Protocol (BGP), MPLS, and IP address resolution as described below.

BGP is a routing information distribution protocol that is designed to define who can talk to whom using multi-protocol extensions and community attributes. VPN membership depends upon logical ports entering the VPN, where BGP assigns a unique route distinguisher. In an MPLS-enabled VPN, BGP distributes forwarding information base tables about VPNs to members of the same VPN. This is designed to permit users to participate on an Intranet and Extranet only if they reside on the correct physical or logical port and have the proper route distinguisher.

A packet received by the network backbone is associated with a particular VPN. A forwarding table associated with the particular VPN is used, along the originating IP address, to determine a set of possible egress interfaces and the packet's IP destination address.

For Customer's with MFS-NBFW on ADI, a GRE tunnel is established between LevelBlue's Security Data Center and the Customer's ADI Plus router located on Customer's premises. Customer's traffic is separated from other Customers' traffic and the defined security policy/firewall configuration applied on the uniquely identified traffic flowing into the MFS - Network Based Firewall platform through the appropriate GRE tunnels.

Overall security and the selection and use of security facilities provided by LevelBlue is a Customer and User responsibility. LevelBlue does not guarantee that use of the security features that LevelBlue provides will prevent unauthorized access to Customer systems or data.

SD–7.2.2. Features of the MSS Network Based Service

Section Effective Date: 17-Nov-2025

MSS Network Based Customers select the Feature Level for their service. This selection pre- determines basic service offering, including number of custom rules and number of included monthly changes (MACD).

Level 1: Outbound Only, Common Customer Security Policy. Only one SDC for egress is allowed under this level. Service Level 1 Includes basic set of reports via the designated LevelBlue Portal. Customers may only choose any or all of the following protocols and ports:

- HTTP (80)
- HTTPS (443)
- HTTP ALT (8080)
- HTTPS ALT (8443)
    - FTP_CTRL (21)
- ICMP ECHO
- DNS UDP/TCP (53)
- TELNET (23)
    - SSH/SFTP (22)

Level 2: Outbound Only, Custom Security Policy (up to 10 rules included). The Customer is only given a single PAT address. If they require more public IP addresses, they must be purchased. Customer may purchase multiple egress SDC's and multiple SecNets. Also, no SMTP Mail Relay is allowed in this Service Level since that assumes inbound traffic.

Level 3: Outbound/Inbound, Custom Security Policy (up to 30 rules included). The Customer by default is assigned a /29 IPv4 address block (with a single PAT and 5 other public IP addresses available where 2 other IPs are reserved for network addresses). If justified the customer may be assigned an additional /29 address block at no additional charge. Any additional IP addresses over the 16 would be chargeable.

Level 4: Outbound/Inbound, Custom Security Policy, up to 50 rules included. The Customer by default is assigned a /29 IPv4 address block (with a single PAT and 5 other public IP addresses available where 2 other IPs are reserved for network addresses). If justified the customer may be assigned 24 additional addresses at no additional charge. Any additional

IP addresses over the 32 total would be chargeable.

Level 5: Outbound/Inbound, Custom Security Policy, up to 99 rules included. The Customer by default is assigned a /29 IPv4 address block (with a single PAT and 5 other public IP addresses available where 2 other IPs are reserved for network addresses). If justified the customer may be assigned 24 additional addresses at no additional charge. Any additional IP addresses over the 32 total would be chargeable.

For NBFW/on ADI: Outbound Only, Custom Security Policy, up to 6 rules included. Customer is given a single PAT address from the ADI address space. One Security Data Center egress is allowed for this offer.

Standard ports:

- HTTP (80)
- HTTPS (443)
- HTTP ALT (8080)
- HTTPS ALT (8443)
    - FTP_CTRL (21)
- ICMP ECHO
- DNS UDP/TCP (53)
- TELNET (23)
- SSH/SFTP (22)

For each of the Levels, LevelBlue MSS-Network Based provides connectivity and security monitoring (both inbound and outbound) that:

- Enables Customers to browse the Internet, logon to remote Hosts (Telnet) and complete file transfers using FTP at high speeds from around the world.
- Restricts access from the Internet into the Customer's corporate network.
- Reduces security risks by employing LevelBlue network security design.
- Provides a variety of access and utilization reports to help monitor Internet usage. LevelBlue MSS-Network Based leverages existing LevelBlue private networks by:
- Installing security features directly into LevelBlue's network. Customer Internet access takes place via a "hub and spoke" arrangement within the LevelBlue packet network. Once Internet- bound traffic reaches the packet network, it is allowed access to the Internet based upon the Customer's specific Security Policy.

SD–7.2.3. Standard Components

Section Effective Date: 28-Feb-2017

For all levels of LevelBlue's MFS-Network Based Service Offer Features:

- Security Monitoring:
  - 7x24 monitoring of traffic into the network Firewall. This keeps inbound attacks outside of the MFS-Network Based infrastructure at the high-throughput circuits, well away from individual Customer components or services.
  - Stateful Inspection of allowed IP traffic via Firewall.
  - Open Systems Interconnection (OSI) Layer 2 isolation. All PVC traffic remains isolated through the MFS-Network Based Service infrastructure and the Security Policy.
- Network:
  - One network as primary defined by the ingress of a single VPN Multi Protocol Label Switching (MPLS network), or as ATM, Internet Protocol enabled Frame Relay (IPeFR) or Internet Protocol enabled Asynchronous Transfer Mode (IPeATM), AVPN or PNT network into a Security Data Center (SDC).
  - If IPeFR, IPeATM, AVPN or PNT are purchased, the MSS-Network Based Service provisions as part of the basic subscription an ePVC (or Logical Channel) and a backup ePVC (or Logical Channel) of the subscribed size into the Service. However, if the Customer is using direct PVC's, then it is their responsibility to provision a backup direct PVC. Note: Only one direct PVC is included in the basic pricing. Additional direct PVC's (primary or backup) are considered additional networks and are charged accordingly.
  - Support for up to 135Mbps per Secnet is provided. Higher bandwidth options are available on an individual case basis.
  - Bandwidth, starting at a minimum of 1.5 Mbps equivalent capacity to support a network up to an equivalent of 135Mbps (higher bandwidths may be available on an individual case basis) on AVPN, EVPN or PNT. For NBFW on ADI, the available bandwidth options are 1.5, 3, 6, 8, 9, 10, 15, 20, 25, 30, 35, 40 or 45Mbps.
  - Any solution requiring a Secnet equal to or over 45Mbps must have Level 4 or higher Feature Level.
  - Transparent, Stateful Inspection (i.e., non-proxied) Internet access
  - Many-to-one outbound network address translation to the Internet, hiding Customer's address space.
- DNS

- DNS services are not provided for the NBFW on ADI Service, but the below details about DNS apply to MSS-NB when the service is provided in conjunction with VPN Multi-Protocol Label Switching (MPLS network), ATM, Internet Protocol enabled Frame Relay (IPeFR) or Internet Protocol enabled Asynchronous Transfer Mode (IPeATM), AVPN or PNT network.
- LevelBlue Primary DNS is provided by LevelBlue-Enhanced Network Services as part of the MSS-Network Based, or it can be provided by a Customers' own DNS authority.
- DNS caching is provided by MSS-Network Based Service to provide Customers with resolution performance and protection services. All Customer queries will be to the MSS-Network Based DNS caching servers from the Customers' specified internal primary DNS servers.
- MSS-Network Based expects that Customers have implemented some form of split DNS, where their internal address resolution resides on an internal corporate root DNS Server for their users' internal address resolution. These internal DNS servers are maintained and administered by the Customer, and will forward external queries to the MSS-Network Based caching DNS servers for resolution.
- MSS-Network Based does not support internal Customer address resolution on its caching DNS servers. The Customer must provide this functionality for its internal network.

- User Authentication
  - If User Authentication is requested to be supported, Customers will be able to set policy controls over User level access to the Internet. After certain criteria is met (as determined by LevelBlue) and needed components are setup in the customer network, the MSS-NB platform will interface with a Customer's hosted and managed User Authentication service (RADIUS, LDAP, or Active Directory) to authenticate User activity to the Internet. (Note: MSS-Network Based will not provision, administer, support or troubleshoot the Customer's User Authentication solution).
  - User Authentication is not available for NBFW on ADI service.
- Intrusion-Detection System (IDS) Logging only
  - MSS-Network Based has implemented a set of certain basic IDS features, which includes limited scanning of Customer traffic for a small number of exploits, attacks and other malicious activities.
  - IDS logging only is available for NBFW on ADI service.
- Self-Administration Capability of NBFW configuration
  - MSS-NB provides a self-administration capability for Customers to

administer certain aspects of the configuration of the MSS-NB solution.
    - For configuration changes unavailable through the self-administration interface, Customers are required to engage the MSS Operations team via the LevelBlue Portal.
- Reporting
    - MSS-Network Based provides reporting via the LevelBlue portal. Content and format of the reports are subject to change without notice. LevelBlue maintains a Customer accessible website where reports may be obtained.

SD-7.2.4. Offer Limitations

Section Effective Date: 28-Feb-2017

- This Service provides Support for up to 10 total authorized Customer contacts (applies to all levels).
- Six (6) MACD service requests per month are allowed with each service level. Additional requests are subject to additional charges (applies to Service Levels 2-5 and Network Based Firewall on ADI).
- One (1) MACD service request per month is allowed for Service Level 1. Additional requests are subject to additional charges.
- No SNMP traffic is allowed to traverse the firewall (applies to all service levels).
- Only Critical ICMP (ping) traffic is allowed (troubleshooting or periodic checks.

Customers are encouraged to aggregate their Rules' source and destination addresses into networks rather than to specific Hosts. Source and destination networks should be subnetted up to the largest/most inclusive range. LevelBlue recommends that source or destination Rules apply to all users (“ANY”), which is usually especially for the common services needed by all users such as HTTP, HTTPS, or FTP.

If a Customer insists on specific granular source addresses, additional MSS-NB address packages can be purchased.

SD–7.2.5. Termination Orders

SD–7.2.5.1. LevelBlue Initiated

Section Effective Date: 23-Jul-2013

LevelBlue may terminate Service Components of MFS-Network Based by giving Customers sixty (60) calendar days' notice.

SD–7.2.5.2. Customer Initiated

Section Effective Date: 23-Jul-2013

If Customer wishes to terminate a MFS-Network Based Service Component, the Customer must provide LevelBlue with at least thirty (30) days' prior written notice to that effect. Recurring monthly charges will continue to apply for a period of at least thirty (30) calendar days from the date when LevelBlue receives a termination notice or until the disconnect date specified in the disconnect order applicable to the affected MFS-Network Based Service Component(s), whichever is later.

SD–7.2.6. Customer Responsibilities

Section Effective Date: 09-Jan-2015

Designating a person who will be the technical focal point to work with LevelBlue to help promote a successful implementation.

- Providing a list of desired IP protocols to deploy during the implementation including source addresses, destination addresses, ports, TCP and/or UDP and a description of the Service to be implemented.
- Providing LevelBlue with user workstation counts and traffic estimates if URL Filtering features or options are selected.
- Providing the necessary network information to allow LevelBlue to provision ingress virtual circuits into the network firewall.
- Identifying a suitable test location during enablement and implementation to properly test desired Security Policies prior to deploying all sites on the MSS-NB Service.
- Utilizing internal Hosts and servers that are properly maintained to include the latest available security patches and are not infected with any worm, trojan or virus

or similar security threat. LevelBlue is not responsible for patching or removing security threats on Customer maintained equipment.

- Ensuring that Customer systems and networks (including outsourced and educational environments) that connect with those belonging to MSS-NB, or that use common services network features, have appropriately implemented security controls. These controls should be designed to prevent loss, disclosure, unauthorized access, or service disruption, by restricting LevelBlue network access and use to authorized Customer personnel only. Use of the LevelBlue network and its facilities is intended for the contracting Customer only and not for those who may be interconnected with the Customer's systems. The administration of
- individual IP addresses on a Customer's LAN, including maintaining distinct, unique, and non-overlapping private IP address space.
- Customer needs to notify LevelBlue about any changes to a Customers configuration(s). If changes to security configurations are necessary at a given location based upon Customer notification, LevelBlue will review these new requirements and make recommendations as necessary.

SD–7.2.7. Service Availability

Section Effective Date: 28-Feb-2017

The MSS-Network Based Service is designed to provide single site redundancy and optional failover to other Security Data Centers in the event of catastrophic failure. Optional failover is not available with NBFW on ADI. LevelBlue incorporates many automatic redundancy and diversity features designed to quickly handle failures in network components. Additionally, equipment within the LevelBlue backbone network and LevelBlue packet services networks are generally connected to other equipment with multiple routes across the global backbone or packet services network infrastructures.

The LevelBlue MSS-Network Based Service is available 7 X 24, except for possible outages during scheduled maintenance. LevelBlue utilizes the scheduled maintenance windows to upgrade equipment, software, and facilities which may add capacity, new features, resiliency and which may provide fixes to known problems to help ensure high network performance. The scheduled maintenance windows are typically used to maintain many sites, including the global backbone, packet services, LevelBlue enhanced network services IDC's and MSS-NB networks. Scheduled maintenance times are:

Scheduled Maintenance Table	
Region	**Times**
United States	Every Sunday - 3:15 a.m. until 4:45 a.m. Eastern Standard Time and every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Canada	Every Sunday - 3:00 a.m. until 4:45 a.m. Eastern Standard Time and every 3rd Sunday* – 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Asia Pacific	Every Monday – 2:00 a.m. until 5:00 a.m. Japan Standard Time and Every 3rd Sunday*- 00:00 a.m. until 8:00 a.m. Japan Standard Time
Europe, Middle East, Africa (EMEA)	Every Sunday – 3:00 a.m. until 5:00 a.m. Central European Time and every 3rd Sunday* - 00:00 a.m. until 8:00a, m. Central European Time
Latin America	Every Sunday - 3:15 a.m. until 4:45 a.m. Eastern Standard Time and every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Note	If the 3rd Sunday of the month falls on a holiday or other special day, LevelBlue may reschedule the monthly maintenance window.

SD–7.2.8. Support and Management

Section Effective Date: 09-Jan-2015

LevelBlue provides the following support for Managed Security Service – Network Based:

SD–7.2.8.1. Initial Consultation for a Customer's Security Enablement

Section Effective Date: 17-Nov-2011

- Review of the inbound and outbound Security Policies provided to LevelBlue by Customer to recommend a proposed migration configuration of the MSS-NB Service.
- Review of the network topology to determine general access requirements.
- Recommendation of Security Policies to meet the current and forecasted needs specified by the Customer, consequent with LevelBlue's need to manage, maintain, operate, and provide measurement reports based upon them.
- Recommendation of additional security management options to meet the specified Customer support needs.

SD–7.2.8.2. Assistance

Section Effective Date: 17-Nov-2011

- Communicating with the Customer's technical contact(s) for installations, moves, adds, or changes.
- Communicating with various LevelBlue work centers for packet services or Managed Router or other data or IP services.

SD–7.2.8.3. Network Monitoring and Management

Section Effective Date: 17-Nov-2011

- Proactive 7x24 monitoring of the Customer's MSS-NB connection (including access) from LevelBlue's network management center of all the components supplied by LevelBlue.

- Help desk support for connection problems related to the MSS-NB service.
- Change management. If changes to security configurations are necessary at a given location based upon Customer notification, LevelBlue will review these new requirements and make recommendations as necessary. LevelBlue will also manage any resulting changes to the platform that LevelBlue deems necessary, which may result in a conversion charge for affected LevelBlue MSS-NB provided Services.
- Scheduled software and hardware maintenance upgrades to help ensure LevelBlue's hardware and software are appropriately configured for transmission of traffic. Problem management, logging, tracking and escalation of reported problems based on LevelBlue specified severity levels.

SD-7.2.8.4. Start Date

Section Effective Date: 17-Nov-2011

The Start Date when a new standard MSS-NB connection will be made available to the Customer will be agreed upon after receipt of a signed contract and/or order letter.

Installation is defined as complete once a Host or other device on a site has been Pinged, a Customer's end-to-end connections have been verified and LevelBlue has implemented the initial deployment of the MSS-NB Service (initial Security Policy deployment).

Billing will begin after successful PING and verification tests are complete, and the initial Customer site(s) have been accepted into maintenance, except in the event that LevelBlue is unable to complete the installation because of Customer actions, including the unavailability of the Customer's final Security Policies or configurations, in which case billing will commence on the original scheduled Start Date.

SD-7.2.8.5. Special Requests

Section Effective Date: 17-Nov-2011

Customers can request a change in bandwidth, optional features and/or functional support (such as service level support) of an installed MSS-NB Service agreement. Other than the possibility of a change in the billing amount, enablement time periods will vary depending on the type of change to the service.

Changes may result in an interruption of connectivity for a period of time depending on the complexity. For each change, LevelBlue will register, arrange for installation, and test

the circuit as appropriate. If required, LevelBlue will configure and arrange for installation of a new network connection (and a backup connection). Additional MSS-NB connection charges may be applied, depending on the type of change to the service.

Change charges are due upon acceptance of an order and payable upon installation or cancellation of an order. Major Service changes or additions may require extended lead times, depending on the type of change. For example, if a Customer's subscription level is increased from 10Mbps to 45Mbps, LevelBlue may require network capacity and packet service resource adjustments.

MSS-NB new connections and migrations are scheduled on an individua l basis. Lead times for installations and changes to existing connections may vary by geography. LevelBlue will endeavor to accommodate special Customer requests regarding installations and conversions such as expediting the scheduled installation date.

LevelBlue will invoice the Customer for engineering or enablement fees plus an administration charge as a result of special requests.

Billing will begin after successful PING and verification tests are complete, and the initial Customer site(s) have been accepted into maintenance, except in the event that LevelBlue is unable to complete the installation because of Customer actions, including the unavailability of the Customer's final Security Policies or configurations, in which case billing will commence on the original scheduled Start Date.

SD–7.2.8.6. Help Desk Support

Section Effective Date: 17-Nov-2011

All problems, questions or requests for assistance related to the MSS-NB Service should be made to the designated LevelBlue help desk support. Problems may be reported by telephone or electronically, where available. The time an incident starts is when a trouble is validated by LevelBlue, and a trouble ticket is opened. The resolution time is the time at which the incident is resolved to the satisfaction of both the Customer and LevelBlue, and the trouble ticket is closed.

- US, EMEA and AP: Centralized Customer Help Centers provide 7x24 problem assistance.

SD–7.2.9. Problem Severity Code Definitions

Section Effective Date: 09-Jan-2015

The Customer defines the severity of a problem when the call is placed. The following definitions are provided as guidance to assist the Customer to appropriately assign the severity of a problem.

Problem Severity Codes and Definitions	
Severity	**Definition**
1	LevelBlue's highest level of severity, a severity 1 Trouble Ticket is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects a Firewall Service Outage. By way of illustration, without any limitation of the description, such incidents include a Firewall Service Component interface(s) being unavailable, any failures of Firewall Equipment and the inability of a Customer sanctioned IP protocol from working through the Firewall Equipment denotes a severity 1 ticket.
2	A severity 2 Trouble Ticket is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects an attack against a Customer's Firewall Equipment. The types of incidents which will generate Severity 2 incidents are: a) unexplained root logins or access attempts to the Firewall, b) unexplained Firewall server file transfers or c) failed or interrupted Firewall processes.
3	Severity 3 Trouble Tickets are defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects certain system health problems with the Firewall Equipment. The types of incidents which will generate Severity 3 alerts are: a) backup problems, such as backup failures or missing backup files, or b) an audit which reveals missing files; or c) Trouble Tickets generated when LevelBlue has specific and accurate information about a specific Customer Trouble.
4	Severity 4 Trouble Tickets are most often used for Moves, Adds and Changes, and Deletes (MACDs). Severity 4 tickets are also generated when LevelBlue needs additional specific information about a Customer Trouble.
5	Severity 5 Trouble Tickets are reserved for changes associated with

	out-of-band testing.

SD-7.2.10. Electronic Problem Reporting

Section Effective Date: 09-Jan-2015

The service hours for electronic problem reporting, available in selected countries, are 24 X 7 excluding the periods for maintenance. LevelBlue will use commercially reasonable efforts to notify Customers in advance of maintenance periods in addition to those listed below. LevelBlue reserves the right to perform emergency maintenance on the electronic Customer support system as may be required.

- United States
  - Saturday 04:00 am EST through Saturday 07:00 am EST
  - Sunday 03:00 am EST through Sunday 05:00 am EST

SD–7.2.11. LevelBlue Managed Firewall Service Network Based Country Availability

Section Effective Date: 09-Jan-2015

The Service is available in select countries in the following regions: a) Americas, b) Asia Pacific ("AP"), c) Europe/Middle East/Africa ("EMEA"), d) Japan, e) United States as detailed in the table below.

In addition, not all service features described in this document are available in all regions and countries. Please refer to the Country Specific Provisions section at the end of the MFS-PB CN Section for additional details.

Table of Regions	
Region	**Countries within a Region**
Americas*	Canada, Netherlands Antilles, Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, Venezuela
Asia Pacific (AP)	Australia, China*, Hong Kong, India, Indonesia*, Malaysia*, New Zealand, Philippines*, Singapore, South Korea, Taiwan, Thailand*
EMEA	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Lithuania, Luxembourg, Latvia, Netherlands, Norway, Poland*, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom
Japan	Japan*
United States	United States
NOTE	Those regions and/or countries marked with an asterisk, the Service is offered on a case by case basis.

SD-8. Glossary

Section Effective Date: 30-Mar-2021

Glossary	
Term	**Definition**
5x8	Means eight (8) hours a day, Monday through Friday of each week, excluding LevelBlue Holidays.
/28	Means 1/16 of a Class C or 16 Host Addresses.
/27	Means 1/8 of a Class C or 32 Host Addresses.
/26	Means 1/4 of a Class C or 64 Host Addresses.
/25	Means 1/2 of a Class C or 128 Host Addresses.
/24	Means 1 Class C or 256 Host Addresses.
Alarm	Means the electronic notification by a monitoring agent that notifies LevelBlue of a possible fault in Customer service as it relates to the MSS services.
Access Control List (ACL)	Means a command on a router to stop specific traffic. An ACL can be configured for a variety of criteria, including layer 2 and layer 3 header information
Advisories	Are those IP Traffic Anomalies that are identified as known attacks (i.e., patches or other defenses are already available, and indicators are that the activity persists at a significant level on the LevelBlue IP Backbone). These are also protocols/services that are purposely monitored due to known or expected IP threats to exploit them (e.g., new vulnerability announced, well-known services such as DNS/HTTP/HTTPS, etc.)
Alerts	Means notification via email or pager of IP Traffic Anomalies or IP Threats that, in the opinion of LevelBlue, require immediate action by the customer to mitigate or to monitor for possible defensive action.
Alert – TMLA	Means an actionable event that elicits a response based on the RP.

Glossary	
Term	**Definition**
Alert Notification	Means the process of providing Alert details to authorized Customer representatives as defined in the IRP.
Appliance NK-Based Managed Firewall Service	Means one of LevelBlue's Managed Security Services described in further detail in this Service Guide that is provided using Resilience-Resilience software capabilities.
Application Firewall Service	Means one of LevelBlue's Managed Security Services described in further detail in this Service Guide.
AT&T Dedicated Internet (ADI)	Means the Internet service provided by and managed by LevelBlue.
LevelBlue Dedicated Internet+ (ADI+)	Means the AT&T Dedicated Internet plus service.
LevelBlue Help Desk	Means the single point of contact for Customer Tier 1 Help Desk(s) regarding the Managed Security Services contained in this Service Guide. The LevelBlue Help Desk will provide the following functions: (i) Manage In-Scope Troubles to Resolution; (ii) Manage the dispatch of LevelBlue personnel to Resolve In-Scope Troubles (iii) perform Soft MACDs; and (iv) Manage the dispatch of LevelBlue personnel to perform Hard MACDs.
LevelBlue IP Backbone	Means the LevelBlue owned and operated Internet Protocol (IP) infrastructure and consists of all LevelBlue Internet Service Points of Presence ("POPs"), the telecommunications Equipment and facilities that interconnect all wiring within them, and the physical plant that surrounds them. The LevelBlue IP Backbone does not include Customer Premise Equipment or the dedicated access facility connecting Customer Premises to the LevelBlue IP Backbone.
LevelBlue Observed Holidays	Means the holidays as defined in the General Provisions.
Attack Mitigation Capability	Is the level of shared scrubbing capacity purchased by Customer from LevelBlue. Scrubbing capacity in a shared packet or non-dedicated environment shall be the capacity of two scrubbing devices.

Glossary	
Term	**Definition**
Attack Mitigation Equipment	Means the denial-of-service detection equipment and the data scrubbing equipment located on LevelBlue's premises and used in connection with the DDoS Service provided to Customer by LevelBlue.
Baseline Service	Means the basic Services described in each of the Managed Security Services sections of this Service Guide. It does not include additional or new Service.
Border Gateway Protocol (BGP)	Means the routing information distribution protocol that is designed to define who can talk to whom using multi-protocol extensions and community attributes.
Capacity-on-Demand	Means the network delivery management functionality.
CERT	Means the Computer Emergency Response Team.
Change Order Process	Means the process by which changes to the Service are requested by Customer and processed by LevelBlue.
Check Point™ Firewall	Means one of the software platforms used to provide LevelBlue's Premises Based Managed Firewall Service.
Choke Router	Means the type of router used to provide LevelBlue's Premises Based Firewall Service.
Committed Information Rate (CIR)	Means the minimum (sometimes guaranteed) throughput for a particular Network element, device, or application.
Client / Endpoint Security Service	Means one of LevelBlue's Managed Security Services described in further detail in this Service Guide.
Connectivity (Front-end and Back-end)	Is how Customer Servers, housed in an IDC, are connected to the Internet and to Customer Premises. Front-end connectivity is how access to the Internet is provided. Back-end Connectivity is Optional as the administrative functions may be performed across the front-end (Internet) connection.

Glossary	
Term	**Definition**
Concurrent Internet Access (also known as “Split Tunneling” or “Dual Access”) capability	Allows packets destined for the Internet to be sent directly to the Internet without passing through the VPN Gateway. LevelBlue will establish an authorization list which will contain all of the IP addresses for VPN Devices that are a part of the Customer’s VPN. If Customer does not request Concurrent Internet Access, the LevelBlue Global Network Client will discard the packets being sent to IP addresses that are not in the authorization list. There is no extra charge for the Concurrent Internet Access option.
Content	Means information made available, displayed or transmitted (including, without limitation, information made available by means of an HTML "hot link", a third party posting or similar means) in connection with a Service, including all trademarks, service marks and domain names contained therein, Customer and User data, and the contents of any bulletin boards or chat forums, and, all updates, upgrades, modifications and other versions of any of the foregoing.
Critical Alert	Means one or more Alerts that require immediate action as defined in the IRP.
Customer Requested Implementation Date	Means the date by which the customer has stated they will begin using the service. The customer had committed to have changed their MX record(s) to direct email to the SEG service by this date.
Customer Signature	Means a signature created to meet a single Customer’s requirement Normal Vendor releases signatures on a bi-weekly basis at least. Sensors will be updated in 3-5 business days at no additional charge to Customer.

Glossary	
Term	**Definition**
Denial of Service Attacks	Means a distributed denial of service attack, similar to those defined in Section SLA-2, directed toward Customer's IP addresses connected to the LevelBlue IP Backbone that, in LevelBlue's reasonable judgment, causes LevelBlue to believe that Customer's network may be compromised by being inundated with nefarious or bogus data traffic, thereby denying service to Customer's systems connected to LevelBlue's IP Backbone.
Domain Name System (DNS)	Means the DNS that translates Internet domain names into IP numbers. A DNS Server is a server that performs this type of translation.
Demilitarized Zone (DMZ)	Means the buffer space outside of both your own and your opponent's direct control. In modern data networks, a Demilitarized Zone is generally an Internet-accessible web, data, or application server that is outside your trusted internal network for use by business partners, Customers, etc. but is not part of the public Internet. DMZs generally allow gated access through passwords or user registration.
Downgrade of Service	Means the change to the service configuration by the customer resulting in a reduction of 10% or more of the monthly recurring charges that were originally contracted in the pricing schedule.
Dynamic Attack Blocking (Shunning)	Means the feature available for Level 2 LevelBlue MIDS Service where the sensor is programmed to dynamically react to serious exploits by managing the screening router to perform this block.
Effective Billing Start Date	Means the first date for which the customer will be billed for the service. This is the same date as the "Customer Requested Implementation Date". However, for those customers that have participated in a SEG trial and then signed this agreement, billing of the service actually begins on the day following the last day of the trial as specified in the SEG trial form.
Emergency Update	Means a signature created for a significant and immediate vulnerability, which will potentially benefit all Customers.

Glossary	
Term	**Definition**
Enhanced Managed Services	Means the enhanced services available for each of the Managed Security Services described fully in this Service Guide.
Event	Means electronic data output from a Customer-defined device that is delivered to the TMLA service for security analysis.
Event Notification	Means the communications between LevelBlue and Customer that relate to identification, Management, and resolution of events, including Outages and any other event that may affect the Service.
Events Per Day (EPD)	Means the average number of Events generated by a device or group of devices within a day.
Forwarding Information Base (FIB) tables	Means the tables that contain information on proper user identification data.
FTP	Means File Transfer Protocol.
GCSC	Means LevelBlue's Global Customer Support Center.
Host-based Intrusion Detection Sensors ("HIDS")	Means the software provisioned on server in Customer's network as it relates to LevelBlue's MIDS. HIDS complements NIDS and provides an option level of security protection for host elements. HIDS provides confirmation of an attack's success or failure, with specific event data (such as user and file name) during an unauthorized access attempt on host or server network components.
Incremental Backup is the Backup	Means to tape of all data files that have changed since the last backup (Full or Incremental), typically performed daily.
In Scope Troubles	Means problems or malfunctions that are LevelBlue's responsibility to resolve as described in this Service Guide.
Install	Means to physically set up for use or service in an IDC, typically associated with HW and SW.
Internet Control Message Protocol (ICMP)	Means the TCP/IP protocol used to report network errors and to determine whether a computer is available on the network. The ping utility uses ICMP.

Glossary	
Term	**Definition**
Internet Data Center (IDC)	Means is the specific LevelBlue facility where Customer Space, HW or Service is located or provided.
Investigation Support	Means to provide root cause analysis information (type of attack, source IP of the attack and what IP address was being attacked) as it relates to LevelBlue's MIDS. Investigation support is available for LevelBlue Level 3 MIDS only.
IP Threat	Refers to data traffic across the LevelBlue IP Backbone such as viruses, buffer overloads, DDoS attacks or other traffic, that may potentially disable, interrupt, or degrade single or multiple connection(s) to the LevelBlue IP Backbone.
IP Traffic Anomaly	Refers to data traffic across the LevelBlue IP Backbone that has a pattern or characteristic recognized by LevelBlue as warranting investigation.
Lightweight Directory Access Protocol (LDAP)	Means the emerging Internet standard for directory services. It is based on the earlier ISO X.500 Directory Access Protocol (DAP) standard, but simplifies that standard considerably, allowing LDAP to be more efficient, straightforward, and easier to implement.
Local Area Network (LAN)	Means a group of computers and associated devices that share a common communications line and typically share resources.
Location	Is each physical customer access location. For example protection of sites at a data center in New York with OC3 access and protection of sites at a data center in Kansas City with separate physical OC3 access would be two locations to be protected.
Mail Exchanger (MX)	Means the domain name server mail exchange record to enable the Secure E-Mail Gateway Service.

Glossary	
Term	**Definition**
MACD (Move, Add, Change, Delete)	Means either Hard or Soft. A Hard MACD is a single HW move, add, change, delete, deactivate, decommission, de-install or disconnect performed by ATT on a single Component Managed by LevelBlue. A Soft MACD is a single logical move, add, change, or delete to the on a Component Managed by LevelBlue.
Managed Intrusion Detection Service (MIDS)	Means the three-level IP network attack recognition and response service and one of LevelBlue's Managed Security Services defined in detail in this Service Guide
Monitoring Services	Is where LevelBlue is using SW integrated to detect WAN, LAN, FW, and Server outages on the Components of the Hosted Infrastructure. For Data Storage Services, this includes disk performance, cache memory usage and related performance metrics.
MPLS	Means multi-protocol label switching.
NetFlow Traffic Data	Means a sample of Customer's data traffic on the LevelBlue IP Backbone used to identify and mitigate DDoS Attack(s).
Network Address Translation (NAT)	Means hiding of IP addresses in an internal network by presenting one IP address to the outside world. It performs the translation back and forth.
Network Elements	Means the Components that make up Customer network and may include items such as Switches, Firewalls, and routers to the Web Servers. They could vary from Client to Client.
Network Intrusion Detection Service (NIDS)	Means the hardware, software, and process solution that provides fully managed and monitored 24 x 7 coverage against network-based security attacks as it relates to LevelBlue's MIDS. NIDS provides real-time for security defense.
Normal	Means the vendor releases signatures on a bi-weekly basis at least. Sensors will be updated in 3-5 business days at no additional charge to Customer.
Outage	Means an interruption of the LevelBlue Managed Security Service, excluding planned maintenance schedules.

Glossary	
Term	**Definition**
PAT or- Port Address Translation	Provides a similar functionality to NAT but is a more specific tool. PAT forwards requests for a particular IP and port pair to another IP port pair.
Permanent Virtual Circuit (PVC)	Is a virtual circuit established for repeated/continuous use between the same data terminal equipment (DTE). In a PVC, the long-term association is identical to the data transfer phase of a virtual call. Permanent virtual circuits eliminate the need for repeated call set-up and clearing.
Personal Data”	Means Data belonging to Customer and its Users which information when taken on its own or in conjunction with other data processed would enable to identify a person.
Planned Event	Means an anticipated increase in the number of requests for Content to Customer’s Web Site on any given day that is equal to or greater than four (4) times the average daily number of requests to Customer’s Web Site during the current month, and that the Customer schedules in advance with LevelBlue.
Premises-Based Managed Firewall Service	Means the suite of Managed LevelBlue Security Services described in this Service Guide.
Pricing Schedule	Means the document that contains the services that Customers can order under the agreement as more fully described in this Service Guide and the prices Customer will pay for such Services.
Pricing Schedule Term	For each Service Component consists of the Pricing Schedule Term for such Service Component for each Service Component consists of the Initial Service Period for such Service Component and all applicable Renewal Periods for such Service Component.
Private Virtual Circuits (PVCs)	Means the circuits used to support LevelBlue’s Network Based Managed Firewall Service.
Proactive Monitoring and Management	Means that LevelBlue is proactively looking into the HW, SW, and connections to verify that the applicable Service is working.

Glossary	
Term	**Definition**
Proactive Operations Support and Troubleshooting	Means LevelBlue will perform tasks that give LevelBlue the ability to take preventive measures to limit the frequency of service Interruptions.
Profiling	Means the analysis completed to determine what alarms are important for a specific Customer as it relates to LevelBlue's MIDS. This profiling is based on Customer's security policy and network infrastructure.
Provisioning Date	Means the date on which the service is enabled by LevelBlue for customer use.
Qualifying Site	Is a specific Customer address identified by Customer to LevelBlue to be monitored by LevelBlue for denial-of-service attacks.
Radius	Means the type of server used to support the provision of LevelBlue's Managed Security Services.
Redundancy	Means the provision of alternate paths to minimize the potential for failure or vulnerabilities.
Remote Client	Means a User connecting to a Server/device from another network.
Resilience-Resilience	Means the brand of hardware used to support LevelBlue's Managed Premise Based Firewall Check Point™ option.
Root Cause Analysis	Determines the origin of any attack and when such attack occurs as it relates to LevelBlue's MIDS.
Router-Based Managed Firewall Service	Means one of LevelBlue's Managed Security Services described in further detail in this Service Guide.
Rules	Means the Customer-defined parameters, thresholds, boundaries, or limitations of a specific Customer's security policy.
S/NOC	Is LevelBlue's Security Network Operations Center.
Server-Based Managed Firewall Service	Means one of LevelBlue's Managed Security Services described in this Service Guide.

Glossary	
Term	**Definition**
Service Activation Date	Means the date the Service becomes available for Customer use.
Service Guide	Means the standard LevelBlue service descriptions and other provisions as revised by LevelBlue from time to time, relating to Service offered under this Attachment. The Service Guide is located at http://www.att.com/abs/serviceguide or at such other address as LevelBlue may specify by posting or email notice.
Service Level Agreement (SLA)	Means the agreement between Customer and LevelBlue to Manage processes, procedures and Equipment pertaining to Customer Service which will reflect a level of performance for LevelBlue to achieve.
Service Outage	Means any occurrence of a failure of service within the LevelBlue IP Backbone, or IDC, or in the Back-end Connectivity. For the LevelBlue IP Backbone, this includes all the Components Managed by LevelBlue in the transmission path from the entrance on the LevelBlue network to where Customer Hosted Infrastructure is located. For the IDC, this includes the Component(s) Managed by LevelBlue in the Hosted Infrastructure and the power and HC/HVAC. For the Back-end Connectivity, this is inclusive of the last Component Managed by LevelBlue. For Customers of LevelBlue Managed and Enhanced Managed Services includes the LevelBlue Equipment used by Customer and Managed by LevelBlue. For Customers of Enhanced Managed Services only, this includes the Back-end Connectivity, up to the last device Managed by LevelBlue, that results in Customer inability to transmit IP packets. A Service Outage does not include any of the events described in Section III.1 of this Service Guide, “General Terms and Conditions Applicable to all Service Level Agreements”, under “Acts or Omissions of Customer or certain Third Parties".

Glossary	
Term	**Definition**
Service Portal	Refers to the website where Customers and User(s) access the Internet Protect Service
Signature Updates	(as related to LevelBlue's MIDS) means the normal Vendor release signatures on a bi-weekly basis, at a minimum. Sensors will be updated in 3-5 business days at no additional charge to Customer. Emergency Update is where a signature created for a significant and immediate vulnerability, which will potentially benefit all Customers. Customer Signature is a signature created to meet a single Customer's requirement
SMTP	Means the type of transfer protocol format used to support LevelBlue's Managed Security Services.
SOCKS	Means the application protocol, as in "The eShield Network Security Appliance sits between the firewall and the company network, scanning all network traffic inbound and outbound, with virus scanning on major protocols including HTTP, FTP, SMTP, News, IMAP, Socks and POP3".
Source Server(s)	Means the device(s) that contain(s) Customer data that LevelBlue copies over to the storage device.
Sun Server	Means the server variety used to provide LevelBlue's Premises Based Managed Firewall Service.
Switch	Means the device that opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits.
System Backup	Means the complete save of all data files and Operating System files – typically performed monthly.
TCP/IP is a Transmission Control Protocol/Internet Protocol	Means the common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide inter-networks. TCP and IP are the two best-known protocols in the suite. TCP corresponds to Layer 4 (the transport layer) of the OSI reference model. It provides reliable transmission of data. IP corresponds to Layer 3 (the network layer) of the OSI reference model and provides connectionless datagram service.

Glossary	
Term	**Definition**
Technical Order Form	Means the technical description of the obligations, duties, or services, including, Equipment Configuration, SW use, and related support services LevelBlue shall provide Customer with before the Service Activation Date.
Technical Interview	Means the first step in the Provisioning Process. It consists of an interview between the LevelBlue ICDS Implementation Manager and the Customer Technical Point of Contact during which Customer shall provide to LevelBlue all technical information reasonably necessary and reasonably requested by LevelBlue.
Telnet	Means the command and program used to login from one Internet site to another. The telnet command/program gets you to the login: prompt of another host.
Time to Respond	Means the time elapsed from the time service outage starts to the time the LevelBlue begins to work the Trouble Ticket.
Tier I Help Desk	Means the function performed by Customer or a third party contracted to Customer to perform initial call receipt, fault validation, or fault isolation. Customer agrees to instruct End-Users to contact the Tier I Help Desk regarding all troubles or questions pertaining to LevelBlue's Managed Security Services. Customer support personnel will make reasonable efforts to Resolve Troubles before they are referred to LevelBlue for Resolution.
Tier II Help Desk	Means the function performed by LevelBlue to receive, Manage, and Resolve Trouble Tickets in accordance with this Service Guide.

Glossary	
Term	**Definition**
Time to Mitigate	For the LevelBlue Internet Protect DDoS Service is defined as the time that LevelBlue takes to initiate mitigation strategies in connection with denial-of-service attacks after attack is detected or after LevelBlue has been notified that the attack is taking place. Time to Mitigate does not include: (1) inability to mitigate a denial-of-service attack type not listed in the above definition of Denial-of-Service Attacks; and (2) inability to mitigate Denial of Service Attacks because the mitigation capacity required exceeds the coverage of Attack Mitigation Capacity purchased by the customer.
Token	With regards to the Internet Protect Service only, shall mean the device, with a built-in computer chip that generates one-time codes (every 60 seconds) that provides the passcode used in two-factor authentication.
Token Authentication	Means the form of two-factor (something you have, something you know) strong authentication.
Traffic Anomaly Detection	Means LevelBlue's identification of Traffic Anomalies directed at a defined set of Customer IP addresses on the LevelBlue Backbone.
Transaction Service Servers	Means any Server other than a Web Servers, which is responsible for responding to the HTTP and HTTPS requests. Typically, Transaction Service Servers are back-end purely Application or Database Servers.
Transition Period for Enhanced Managed Services ordered under the Managed Security Services Service Order Attachment	Means the time period between the Implementation Date and the Production Ready Date.
Trouble Ticket	Means the work order that LevelBlue uses to identify In-Scope and Out of Scope Troubles and to Manage the In-Scope Troubles through Resolution.

Glossary	
Term	**Definition**
Tuning	Means the disabling or setting specific thresholds for signatures to eliminate alarms which have no value to Customer's security policy or infrastructure.
Turnkey	Means the system for which LevelBlue provides the end-to-end service capabilities for a Customer.
UAT (User Acceptance Test) for Enhanced Managed Services	Means the User Acceptance Test, conducted by Customer and LevelBlue.
UDP is a User Datagram Protocol	Means one of the protocols for data transfer that is part of the eTCP/IP suite of protocols. UDP is a stateless protocol in that UDP makes no provision for acknowledgement of packets received.
Uninterruptible Power Supply	Means the backup power device or system that allows Servers to continue running for a limited time when the primary power source is lost.
Verifiable Trouble Tickets	Means the tickets whereby LevelBlue has substantiated that an Outage or other failure to meet the guarantees set forth herein has occurred.
VCCs	Are like Frame Relay Permanent Virtual Circuits except they travel across an Asynchronous Transfer Mode (ATM) network.
VPN Access	Means the highly secured access to the Staging Server via the Virtual Private Network (VPN), which is a highly secure connection over the Internet, and only Customer Authorized Users can access them,
Websense	Means the dynamic URL screening based on access control to Internet sites.

Service Level Agreements (SLA)

SLA-1. Premises Based Services (including PBFW, HIDs, Proxy and MIDs) Maintenance and Support Service Level Targets

Section Effective Date: 01-Oct-2014

Site Configuration	*Metric*	Performance Objective
Single standalone (SA)	MTTR	Repair 90% of Severity 1 Incidents not requiring dispatch within 2 hours of Trouble Ticket generation
	MTTR	Repair 90% of Trouble Tickets requiring 1 dispatch within 8 hours of Trouble Ticket generation
	MTTR	Repair 90% of Customer generated Trouble Tickets not requiring dispatch within 4 hours of Trouble Ticket generation
	MTTR	Repair 90% of administration Trouble Tickets within 8 hours of Trouble Ticket generation
	Availability	99.90%
	MACD	99% - Mean Time to Implement MACD Orders
	Implementation	Within next Business Day
	Client Notification	90% - Time in which LevelBlue will provide notice to Customer of an “auto-detect” Trouble Ticket within 15 minutes of Trouble Ticket generation

Site Configuration	*Metric*	Performance Objective
High Availability (HA)	*MTTR*	Repair 99% of Severity 1 Incidents not requiring dispatch within 2 hours of Trouble Ticket generation
	MTTR	Repair 99% of Trouble Tickets requiring 1 dispatch within 8 hours of Trouble Ticket generation
	MTTR	Repair 99% of Customer generated Trouble Tickets not requiring dispatch within 4 hours of Trouble Ticket generation
	MTTR	Repair 99% of administration Trouble Tickets within 8 hours of Trouble Ticket generation
	Availability	99.999%
	MACD Implementation	99% - Mean Time to Implement MACD Orders within next Business Day
	Client Notification	90% – Time in which LevelBlue will provide notice to Customer of an “auto-detect” Trouble Ticket within 15 minutes of Trouble Ticket generation

SLA-2. LevelBlue Secure E-Mail Gateway Service Level Agreement

SLA-2.1. Network Uptime SLA – 99.999%

Section Effective Date: 17-Nov-2011

Description: The percentage of time in a calendar month that the network is able to receive and process email messages.

- Includes emergency and planned maintenance

SLA Remedy		
Description	**% of Service Availability per Calendar Month**	**Service Credit**
SEG Network Uptime SLA	<99.999%	25%
	<99.0%	50%
	<98.0%	100%

SLA-2.2. Email Latency of 1 Minute or Less

Section Effective Date: 17-Nov-2011

Email delivery is defined as the elapsed time from when an email enters the SEG network to when the delivery attempt is first made.

Email delivery latency is the average of total email delivery time measured in minutes over a calendar month. Email delivery time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.

Email delivery latency applies only to legitimate business email (non-bulk email) delivered to valid email accounts.

This SLA shall not apply to:

- Delivery of email to quarantine or archive
- Email in deferral queues
- Denial of Service attacks (DoS)
- Email loops

SLA		
SLA	**Average Email Delivery Time**	**Service Credit**
SEG Latency SLA	Greater than 1 minute	25% of the Monthly Recurring Charges
	Greater than 4 minutes	50% of the Monthly Recurring Charges
	Greater than 10 minutes	100% of the Monthly Recurring Charges

SLA-3. DDoS Service Level Agreements and Objectives

SLA-3.1. Attack Types and Descriptions

Section Effective Date: 17-Nov-2011

Attack Types and Descriptions	
Attack Type	Description
Spoofed	Sending packets with a forged source address
Malformed	Sending packets with abnormal bits or flags set
Floods	Sending high rates of legitimately formed packets
Null	Sending packets with no content or illegitimate protocol
Fragmented	Sending packet fragments that will never be completed
Brute Force	Sending packets that exceed defined flow rates threshold

SLA-3.2. Overview

Section Effective Date: 17-Nov-2011

Service Level Agreements ("SLAs") are available only for the DDOS Service and no other AIP service options. Failure of the DDOS Service to meet the SLAs described below may entitle Customer to receive credits, as indicated below. Service Level Objectives ("SLO") are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

SLA-3.3. Service Level Agreement Rules, Regulations and Limitations

- *Section Effective Date: 06-Jun-2024*

- The SLAs apply only to the LevelBlue Internet Protect DDoS Service specified in the applicable SLA description and to no other services or options.
- Customer must proactively submit an SLA claim in writing and request the credit within 30 days of the incident in order for this SLA to take effect or forfeit their right to the claim. All credit requests should be sent via an email addressed to budsock@att.com or such other email address identified by LevelBlue, or via U.S. Postal Mail to the following address:

LevelBlue Enterprises, LLC

Attn: LevelBlue Internet Protect SLA

Manager One LevelBlue Way, Room 3A184

Bedminster, NJ 07921

Please include the Trouble Ticket number with your request. LevelBlue will attempt to acknowledge all requests for credit within 10 business days of receipt and inform customer via email or U.S. Postal Mail within 30 days whether the request is approved or denied.

- Trouble tickets, where the Time to Mitigate cannot be verified with LevelBlue's standard diagnostic procedures, do not count towards these SLAs.
- The SLAs will take effect upon the Service Activation Date of the DDoS Service.
- The monthly service charge that will be the subject of the credit for the DDoS Service will be the monthly charge for the Service.
- LevelBlue will only be responsible for a DDoS related attack in which the offending traffic can be routed to the LevelBlue access link with Customer. In the event that

the Customer's traffic (or any portion thereof) is not routed through LevelBlue these SLA will not apply. The SLAs do not apply and no credits will be issued in the event of:

- fire, explosion, lightning, power surges or failures, strikes or labor disputes, water, acts of God, the elements, war, civil disturbances, acts of civil or military authorities, fuel, or energy shortages, acts or omissions of suppliers or other causes beyond LevelBlue's control, whether or not similar to the foregoing, and acts outside LevelBlue's control as described in Section 8 of the LevelBlue Master Agreement
- Local or international regulatory laws or ethical (ethical meaning conforming to accepted professional standards of conduct) issues that limit or prevent the ability of LevelBlue or the Local Service Provider to offer or comply with these SLAs
- Customer's failure to provide required site power for necessary equipment, including the Customer edge router and Channel Service Unit/Digital Service Unit
- Customer's lack of availability to respond to incidents that require Customer's participation for resolution.
- Any service failure which is due to Customer owned equipment residing on Customer's premises (unless such equipment was provided by LevelBlue or its authorized contractors), or failure or unavailability of any of the elements of the services provided by Customer or under Customer's responsibility including, but not limited to, power supply, internal wiring, proper environmental conditions, or router connected telephone line for problem determination.
- Any service failure or interruption caused by a third party (including LevelBlue subcontractors, suppliers, and Local Service Providers) not recognizing or delivering upon an LevelBlue request to reroute a customer's traffic to LevelBlue's designated facilities for the purpose of scrubbing the traffic,
- Scheduled maintenance. LevelBlue will perform maintenance during the scheduled maintenance window of 1 a.m. U.S. Eastern Standard Time (06:00 UTC) to 5 a.m. U.S. Eastern Standard Time (10:00 UTC). LevelBlue may perform maintenance outside of the scheduled maintenance window upon an advanced prior notice to the customer. LevelBlue reserves the right to provide emergency maintenance, or to repair services, at any time and when LevelBlue determines needed, and in such case LevelBlue will notify affected customers as soon as is reasonably practicable. SLAs do not apply during

any of the maintenance periods.

- All claims are subject to review and verification by LevelBlue.
- LevelBlue reserves the right to change or modify the terms and conditions or discontinue this SLA program at any time without notice.
- Credit amounts are calculated based on billed charges, exclusive of any applicable taxes charged to the customer or collected by LevelBlue.
- The SLAs are also subject to the terms and conditions of the service agreement (also referred to as Master Agreement or Agreement).
- The SLA credits may not under any circumstances exceed (either alone or in combination with other credits issued to Customer) in any given month, 100% of the LevelBlue Internet Protect Service monthly charges for DDoS Defense option, for each Qualifying Site.
- The SLAs are Customer's sole and exclusive remedy for any outages, failures of the Service or LevelBlue otherwise not meeting the Service Level Agreements outlined herein.

SLA-3.3.1. Time to Mitigate Service Level Agreement

SLA-3.3.1.1. Service Level Measure

Section Effective Date: 08-Jul-2013

Attack Notification within 15 minutes of identification.

- If the Customer chooses automatic Attack Mitigation: Mitigation begins within 30 minutes of attack identification
- If the Customer chooses to concur before Attack Mitigation: Mitigation begins within 30 minutes of Customer agreement.

If in any calendar month LevelBlue fails to meet the service level measures set forth above in connection with one or more distributed denial of service attack(s) of the type set forth in the Definitions below, and subject to the limitations set forth in section 2.3.1.2, "Service Level Agreement Rules, Regulations and Limitations" Customer may be eligible for a credit equal to a percentage of the total monthly charge, based on Time to Mitigate table below. This SLA will be calculated based on LevelBlue trouble tickets indicating the failure time identified on the ticket(s).

Time to Mitigate	
Time to Mitigate (in minutes	Percentage of Monthly Charge Credit
31-60	25%
61-120	50%

SLA-3.3.1.2. Time to Mitigate Additional SLA Rules, Regulations and Limitations

Section Effective Date: 17-Nov-2011

The duration of time to mitigate will be determined by using the log information from the Attack Mitigation Equipment or trouble tickets logged with the appropriate LevelBlue Customer Care organization. If the latter is used, the time starts with the opening of a trouble ticket by LevelBlue Customer Care and ends when LevelBlue Customer Care sends notification to Customer of the restoration of the Service.

SLA-4. Service Level Objectives

SLA-4.1. LevelBlue Managed Firewall Service – Premises Based Service Level Objectives — Enterprise configuration (does not apply to Standard or Premium configuration Service)

Section Effective Date: 23-May-2016

Meantime to Repair (MTTR) objectives

- LevelBlue has the following meantime to repair targets for the MFS-PB service:
  - Repair 90% of Severity 1 Incidents not requiring dispatch within 4 Hours of ticket generation
  - Repair 90% of tickets requiring 1 dispatch within 8 Hours of ticket generation
  - Repair 90% of Customer generated tickets not requiring dispatch within 4 Hours of ticket generation,
  - Repair 90% of administration tickets within 8 Hours of ticket

generation Notes: the onsite service level target is measured from the

time of fault isolation

- Moves / Adds / Changes (MAC's) objectives:
  - It is LevelBlue's' objective to implement 99% of MAC's within next business day.
- Call Answer objectives:
  - It is LevelBlue's objective to answer client calls to the Security Network Operations Center within 30 seconds

SLA-4.2. LevelBlue Managed Firewall Service – Network Based Service Level Objectives

Section Effective Date: 20-Jan-2012

LevelBlue will observe the following objectives when delivering MSS-NB:

- Implementing Change Requests - MACD turnaround time of 24 hours
- Service Availability - 99.99%

SLO-0.1. LevelBlue Managed Intrusion Detection Service Level Objectives

Section Effective Date: 29-Mar-2013

Managed Intrusion Detection Performance Objective Table	
Site Configuration	Performance Objective
Single standalone	99.9%
High Availability ("HA") active/standby or active/active	99.999%

Managed Intrusion Detection Mean Time to Repair Performance Objective Table	
Site Configuration	**Performance Objective**
Single standalone	Repair 90% of Severity 1 incidents not requiring dispatch within 2 hours of Trouble Ticket generation
	Repair 90% of Trouble Tickets requiring 1 dispatch within 8 hours of Trouble Ticket generation
	Repair 90% of Customer generated Trouble Tickets not requiring dispatch within 4 hours of Trouble Ticket generation
	Repair 90% of administration Trouble Tickets within 8 hours of Trouble Ticket generation
High Availability ("HA") active/standby or active/active	Repair 99% of Severity 1 incidents not requiring dispatch within 2 hours of Trouble Ticket generation
	Repair 99% of Trouble Tickets requiring 1 dispatch within 8 hours of Trouble Ticket generation
	Repair 99% of Customer generated Trouble Tickets not requiring dispatch within 4 hours of Trouble Ticket generation
	Repair 99% of administration Trouble Tickets within 8 hours of Trouble Ticket generation

Managed Intrusion Detection Mean Time to Implement MACD Orders Performance Objective Table	
	Performance Objective
Mean Time to Implement MACD Orders: within next business day	99.0%

Managed Intrusion Detection Time to Notify Performance Objective Table	
	Performance Objective
Instances in which LevelBlue will provide notice to Customer of an "auto-detect" Trouble Ticket within 15 minutes of Trouble Ticket generation	99.0%

Pricing (P)

P-1. LevelBlue Managed Firewall Service (Premise Based) Router Based (MFS-RB) Service Charges

Section Effective Date: 17-Nov-2011

Customer's use of the MFS-RB Service will incur some or all of the following types of charges:

- One-time installation charges:
  - Basic service charge
  - Optional DMZ interface feature installation charge
- Monthly recurring charges:
  - Basic service charge

The above monthly recurring charges are pro-ratable, and the above one-time installation and conversion charges are not pro-ratable.

LevelBlue Managed Firewall Service (Premises Based) – CS Option (Server Based

P-2. LevelBlue Managed Firewall Service (Premises Based) – CS Option (Server Based) (MFS- PB CS Option) Service Charges

Section Effective Date: 17-Nov-2011

MFS-PB CS Option charges are incurred for the service components that support the attachment of Customer systems to service and for those features of the Services offered by LevelBlue.

Customer use of MFS-PB CS Option may incur some or all of the following types of charges:

- One-time installation charges:
  - Basic Service Charge.
  - Optional feature installation and set-up charges including but not limited to URL filtering, VPN Support, User Authentication support, HA or 7x24x4 (four-hour response time) for onsite support.
  - Adding an optional feature or increasing the service level of any feature to the next user or support level.
- Monthly Recurring Charges:
  - Basic Service Charge.
  - Optional feature charges including but not limited to URL filtering, VPN

support, user authentication, additional Secure Networks, HA or 7x24x4 onsite support.
- Custom Service enhancements as agreed upon by the Customer, product management, development and other LevelBlue enablement, support, or maintenance groups.
- Conversion charges as applicable when current Service is being upgraded, downgraded, or changed.

The above monthly recurring charges are prorated and the above one-time installation and conversion charges are not prorated.

P-3. LevelBlue Managed Premises-Based Firewall Service– CN Option (Appliance Based) (MFS-PB CN Option) Service Charges

Section Effective Date: 21-Mar-2012

MFS-PB CN charges are incurred for components that attach Customer systems to the MFS-PB CN Service and features.

The Customer's use of MFS-PB CN will incur some or all of the following types of charges:

- One-time Installation Charges:
  - Basic service charge based on type of device and number of users.
  - Optional feature installation charges as listed above.
  - Custom service enhancements as agreed upon by the Customer and LevelBlue.
  - Optional feature charges selected, including but not limited to HA.
  - Adding an optional feature or increasing the level of any feature to the next user or support level.
- Monthly Recurring Charges:
  - Basic service charge based on number of users and type of device deployed.
  - Optional feature charges including VPN support, user authentication, additional highly secure networks.
  - Custom service enhancements as agreed upon by the Customer and LevelBlue.
  - Optional feature charges selected, including but not limited to HA.
  - Conversion charges as applicable when current Service is being upgraded, downgraded, or changed.

The above monthly recurring charges are prorated and the above one-time installation and conversion charges are not pro-ratable.

P-4. LevelBlue Managed Premises-Based Firewall Service — CP Option (HW/SW Solution) Service Charges

Section Effective Date: 17-Nov-2011

Customer use of MFS-PB CP Option will incur some or all of the following types of charges:

- One-time installation charges:
  - Basic Service Charge
  - Optional feature installation and set-up charges including but not limited to VPN support, user authentication support, and/or DMZ/Extranet.
  - Custom Service enhancements, which are agreed upon by the Customer and LevelBlue.
  - Adding an optional feature.
- Monthly Recurring Charges:
  - Basic Service Charge.
  - Optional feature charges including but not limited to VPN support, user authentication support, and/or DMZ/Extranet.
  - Custom Service enhancements as agreed upon by the Customer, product management, development and other LevelBlue enablement, support, or maintenance groups.
  - Conversion charges as applicable when current Service is being upgraded, downgraded, or changed.

The above monthly recurring charges are prorated, and the above one-time installation and conversion charges are not prorated.

P-5. LevelBlue Managed Network-Based Firewall Service Charges

Section Effective Date: 21-Mar-2012

Use of LevelBlue Managed Network-Based Firewall will incur some or all of the following types of charges:

- One-time installation charges:
  - Basic service charge based on bandwidth (subscription level)
  - Optional feature installation charges including URL Filtering, User Authentication, additional highly secure networks

- Custom Service enhancements as agreed upon by the Customer, product management, development and other LevelBlue enablement, support, or maintenance groups
- Optional feature charges selected, for example multiple site backup or failover.

- Move, add, or change of the service to include:
- Increasing subscription level after the initial Service is enabled
- Adding an optional feature or increasing the service level of any feature to the next user or support level
- Monthly Recurring Charges:
- Service charge based on bandwidth (subscription level)
- Optional feature installation charges including URL Filtering, additional highly secure networks, or other billable features
- Custom Service enhancements as agreed upon by the Customer, product management, development and other LevelBlue enablement, support, or maintenance groups
- Optional feature charges selected, for example multiple site backup or failover.
- Conversion charges as applicable when current Service is being upgraded, downgraded, or changed.

The above monthly recurring charges are prorated, and the above one-time installation and conversion charges are not prorated.

P-6. LevelBlue Managed Intrusion Detection Service Charges

Section Effective Date: 17-Nov-2011

The following charges are applicable for all MIDS Levels:

- One-time set-up
- Monthly recurring charge

LevelBlue MIDS Levels 1 and 2 includes equipment supplied by LevelBlue. MIDS Level 3 is flexible in that equipment can be included as a custom option, or if a Customer currently owns IDS sensors LevelBlue will monitor them provided they comply with LevelBlue's current hardware and software requirements.

P-7. LevelBlue Token Authentication Service Charges

Section Effective Date: 17-Nov-2011

Pricing elements for LevelBlue Token Authentication Service include:

- A one-time license charge per Customer
- An annual license maintenance charge (which may vary based on the number of token/RSA Authentication Manager Servers)
- A one-time charge per token (for the cost of the tokens)
- A monthly recurring management charge for each active token
- Shipping charges for tokens

Contracts are available for a term of 24, 36, 48, and 60 months. The minimum term is 24 months. A minimum of 25 users is required.

Country-Specific Provisions (CSP)

CSP-1. LevelBlue Managed Premises-Based Managed Firewall

CSP-1.1. General terms for Asia Pacific (AP) and Europe, Middle East, and Africa (EMEA)

Section Effective Date: 09-Jan-2015

In AP and EMEA the Services are part of the LevelBlue Managed IP Security Services portfolio.

CSP-1.2. Access

Section Effective Date: 02-Mar-2017

In AP and EMEA the service is sold in combination with AT&T Dedicated Internet Global service (ADIG) and LevelBlue Virtual Tunneling Services – Site-to-Site VPN, or 3rd Party ISP services.

CSP-1.3. Helpdesk support

Section Effective Date: 09-Jan-2015

- Asia Pacific: During office hours local language and English are supported
- EMEA: During office hours the following 6 languages are supported: Dutch, English, French, German, Italian and Spanish
- Outside office hours support is given in English on a 24x7 basis

CSP-2. LevelBlue Managed Premises-Based Firewall (Router Based)

Section Effective Date: 09-Jan-2015

MFS-RB Service is available only in the United States.

CSP-3. LevelBlue Managed Premises-Based Firewall – CS Option (Appliance Based) (MFS-PB CS Option)

Section Effective Date: 09-Jan-2015

MFS-PB CS Option Service is available only in the United States

CSP-4. LevelBlue Managed Premises-Based Firewall – CN Option (Appliance Based) (MFS-PB CN Option)

Section Effective Date: 09-Jan-2015

Except where specifically defined in a contract addendum, the MFS-PB CN option is available in the United States, EMEA and AP countries where LevelBlue has a presence. Other country implementations and terms will be made available as needed on an individual case basis.

CSP-4.1. General terms for AP and EMEA

CSP-4.1.1. Access

Cross references

CSP-1.2 Access

CSP-4.1.2 Country Specifics within Asia Pacific

Section Effective Date: 09-Jan-2015

Asia Pacific will have only limited countries where the service is available. Service is part of the LevelBlue IP Security Services Portfolio and is available in Australia, Hong Kong, New Zealand, Singapore, and Taiwan.

CSP-4.1.2.1. Australia

CSP-4.1.2.1.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one-year starting from the Service Activation Date.

CSP-4.1.2.1.2. Charges

CSP-4.1.2.1.2.1. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount outstanding, at the rate of two (2) percent per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non- payment can result in disconnection.

CSP-4.1.2.2. Hong Kong

CSP-4.1.2.2.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one-year starting from the Service Activation Date.

CSP-4.1.2.3. India

CSP-4.1.2.3.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one-year starting from the Service Activation Date.

Customer understands that it must comply with the unique terms and conditions as specified in Customer's Pricing Schedule.

CSP-4.1.2.4. New Zealand

CSP-4.1.2.4.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-4.1.2.5. Singapore

CSP-4.1.2.5.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-4.1.2.5.2. Charges

CSP-4.1.2.5.2.1. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount outstanding, at the rate of 2% per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non-payment can result in disconnection.

CSP-4.1.2.6. Taiwan

CSP-4.1.2.6.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-4.1.2.7. South Korea

CSP-4.1.2.7.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Access Connection shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-4.1.2.7.2. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount outstanding, at the rate of 2% per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non-payment can result in disconnection.

CSP-4.1.3. Country Specifics within EMEA CSP-4.1.3.1. Germany

Section Effective Date: 09-Jan-2015

We provide and pay for the dial telephone connection which allows us to connect a diagnostic modem which we provide.

CSP-4.1.3.2. Netherlands

Section Effective Date: 09-Jan-2015

The dial telephone connection for the asynchronous modem for remote problem determination and the cabling to connect it to the router we provide is included with the managed access connection when provided by LevelBlue.

CSP-4.1.3.3. Italy

Section Effective Date: 09-Jan-2015

The dial telephone connection line for the asynchronous modem which is provided for remote problem determination must be provided by LevelBlue Global Network Services Italia S.p.A due to PTT rules and an additional charge applies to you.

CSP-4.1.3.4. United Kingdom

Section Effective Date: 09-Jan-2015

The dial telephone connection for the asynchronous modem for remote problem determination and the cabling to connect it to the router we provide is included with the managed access connection when provided by LevelBlue.

CSP-5. LevelBlue Managed Firewall Service (Premises Based) — CP Option (HW/SW Solution)

Section Effective Date: 09-Jan-2015

MFS-PB CP Option is available only in the United States.

CSP-6. Managed Firewall Service — Network Based (MSS-NB)

CSP-6.1. General terms for AP and EMEA

Section Effective Date: 09-Jan-2015

In AP and EMEA the Service is part of the LevelBlue Managed IP Security Services portfolio.

CSP-6.1.1. EMEA Help Desk Support

Section Effective Date: 09-Jan-2015

- Asia Pacific: During office hours local language and English are supported
- EMEA: During office hours the following 6 languages are supported: Dutch, English,

French, German, Italian and Spanish
- Outside office hours support is given in English on a 24x7 basis

CSP-6.1.2. Country Specifics within Asia Pacific

Section Effective Date: 09-Jan-2015

Asia Pacific will have only limited countries where the service is available. Service is part of the LevelBlue IP Security Services Portfolio and is available in Australia, Hong Kong, New Zealand, Singapore, and Taiwan.

CSP-6.1.2.1. Australia

CSP-6.1.2.1.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one-year starting from the Service Activation Date.

CSP-6.1.2.2. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount outstanding, at the rate of two (2) percent per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non- payment can result in disconnection.

CSP-6.1.2.3. Hong Kong

CSP-6.1.2.3.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one-year starting from the Service Activation Date.

CSP-6.1.2.4. India

Section Effective Date: 09-Jan-2015

Customer understands that it must comply with the unique terms and conditions as specified in Customer's Pricing Schedule.

CSP-6.1.2.5. New Zealand

CSP-6.1.2.5.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-6.1.2.6. Singapore

CSP-6.1.2.6.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-6.1.2.6.2. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount

outstanding, at the rate of 2% per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non-payment can result in disconnection.

CSP-6.1.2.7. Taiwan

CSP-6.1.2.7.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Firewall Service shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-6.1.2.8. South Korea

CSP-6.1.2.8.1. Service Activation Date

Section Effective Date: 09-Jan-2015

Any Managed Access Connection shall be provided to Customer for a minimum service period of one year starting from the Service Activation Date.

CSP-6.1.2.8.2. Late Payment Charges

Section Effective Date: 09-Jan-2015

Payment will be due thirty (30) days from invoice date. If payment is not received within thirty (30) days from invoice date, a late payment fee will be applied on the amount outstanding, at the rate of 2% per month, calculated on the number of days the payment is received late. At the end of each month, an invoice for late payment fee will be generated; and a final invoice will be issued for additional late payment fee based on the exact date of payment. Non-payment can result in disconnection.

CSP-6.1.3. Country Specifics within EMEA

Section Effective Date: 09-Jan-2015

None

CSP-7. Managed Intrusion Detection Service

CSP-7.1. General

Section Effective Date: 09-Jan-2015

MIDS Level 2 and Level 3 is available in US and Internationally, with service availability in the following countries with support through LevelBlue's Network Integration - Global Customer Solutions: Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, and the UK.

CSP-7.1.1. Provision of IP address information

Section Effective Date: 09-Jan-2015

The provision of IP address information to the Customer by LevelBlue, either via MIDS reporting or problem determination processes, is subject to restrictions imposed by European and country legislation.

CSP-7.1.2. EMEA specific terms

Section Effective Date: 09-Jan-2015

The following specific terms apply instead of those terms identified elsewhere in this Service Guide:

CSP-7.1.2.1. Service Features

Section Effective Date: 09-Jan-2015

Implementation of up to 5 unique ID signatures per sensor, and traffic direction to be defined by LevelBlue, including their prior validation by Customer, in response to anticipated or actual security threats.

CSP–7.1.2.2. Customer Responsibilities

Section Effective Date: 09-Jan-2015

Regular Vendor Signature updates:

The alarm level setting of all new signatures or their updates concerned will be communicated by LevelBlue, via e-mail, allowing Customer to decide and communicate to LevelBlue which alarm level setting Customer wants to effectively apply; in the absence of a communication by Customer to LevelBlue, via e-mail, within 2 business days, Customer agrees hereby that the alarm level settings in place for such new signatures or their updates are duly decided by Customer and part of the business risks undertaken by Customer.

- Provided it has been agreed upon beforehand between Customer and LevelBlue, emergency updates implemented within 24 hours or earlier based on severity and verification by LevelBlue. The alarm level setting of these updates concerned will be communicated by LevelBlue, via e- mail, allowing Customer to decide and communicate to LevelBlue which alarm level setting Customer wants to effectively apply; in the absence of a communication by Customer to LevelBlue, via e-mail, within 2 business days, Customer agrees hereby that the alarm level settings in place for such new signatures or their updates are duly decided by Customer and part of the business risks undertaken by Customer.
- LevelBlue being the Customer's subcontractor, Customer is solely responsible for determining the actions to be implemented for, including the related consequences of, the operation of the intrusion detection provided by the MIDS functionalities and Service, including obtaining, as required by applicable laws, all consents of all persons whose data, of whatsoever kind, would be processed, or rights would be affected, at the occasion of, or for each of the purposes of this LevelBlue MIDS service, including the latter's activities performed by LevelBlue or the Customer as described in this Service Guide or the Agreement. For pursuing any other purpose, not mentioned under this Service Guide or Agreement, the Customer acknowledges to be solely responsible for such purposes and warrants to act in accordance with applicable laws. In all these circumstances, Customer commits to keep LevelBlue, its officers or directors and employees or subcontractors, harmless and free from any action, recourse or claim for damages or requests for other payments.
- Customer is solely responsible, upon basis of his own security policies and business posture and risks pursued, to decide upon, including to communicate to LevelBlue, the alarm level settings retained by Customer for each signature provided by the

Vendor from whom LevelBlue procures the Managed Intrusion Detection System and tools. To this effect, Customer agrees to undertake the obligation to research, compile and analyze any dissemination of general security information, including instant alerts or security advisories, relating to threats and/or anomalies, such as for example on virus infections or whatsoever attacks, which may affect networks and which is made available, for free or for a fee, by other sources publicly available on the Internet.

CSP-8. LevelBlue Token Authentication Service

CSP-8.1. US

Section Effective Date: 09-Jan-2015

Billing is in US currency.

CSP-8.2. General terms for EMEA

Section Effective Date: 09-Jan-2015

In EMEA the Service is part of the LevelBlue Managed IP Security Services portfolio. Subscription Solution is generally available in EMEA. Dedicated Solution is available on Individual Case Basis only.

CSP-8.3. Billing

Section Effective Date: 09-Jan-2015

EMEA Billing is in local currency

CSP-9. LevelBlue Internet Protect Service

CSP-9.1. Argentina

CSP-9.1.1. Billing and Payment Currency

Section Effective Date: 13-Jan-2021

This provision can be found in the General Provisions.

CSP-9.2. Brazil

CSP-9.2.1. Billing and Payment Currency

Section Effective Date: 13-Jan-2021

This provision can be found in the General Provisions.

CSP-9.3. Canada

CSP-9.3.1. Web Based Billing

Section Effective Date: 13-Jan-2021

Unless Customer receives invoices through LevelBlue's Consolidated Statement Facility, Customer agrees that LevelBlue may deliver invoices solely by enabling Customer to access them via the LevelBlue Web Based Billing facility. LevelBlue will enable Customer to access this facility with a User ID and password. Customer must provide LevelBlue with the name, telephone number, email, and mail addresses of the designated billing contact for this purpose. LevelBlue will notify the designated billing contact by email when monthly invoices are posted to the LevelBlue Web Based Billing facility. Customer agrees to check the LevelBlue Web Based Billing facility at least once monthly for current invoices posted whether or not Customer has received the email notification. Customer agrees that Customer will be deemed to have received each such invoice as of the date it is posted and that failure on Customer's part to access any invoice shall not relieve, waive, or delay the obligation to promptly pay charges incurred. Customer must give notice in writing immediately should Customer change the designated billing contact including the new designated billing contact's name, telephone number, email, and mail addresses, by email at agnscanada@att.com or fax (905-762-7410).

CSP-9.4. Chile

CSP-9.4.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

LevelBlue will invoice all applicable charges in local currency. The charges, which are quoted and contracted in US Dollars, will be converted to local currency using the exchange rate issued by the Banco Central de Chile on the invoice date.

CSP-9.5. Colombia

CSP-9.5.1. Charges

Section Effective Date: 09-Jan-2015

Unless otherwise mandated by Colombian law, invoices for all applicable charges shall be rendered in US Dollars, and payment shall be made in US Dollars. If any law, rule, or regulation of a competent Colombian authority requires that payment for services rendered in Colombia must be made in Colombian Pesos, payment shall be made in the equivalent amount in Colombian Pesos based on the official exchange rate or "Tasa Representativa del Mercado" ("T.R.M."), set on the day immediately prior to the date the payment is made.

CSP-9.6. Ecuador

CSP-9.6.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

Invoices shall be rendered in US Dollars and charges shall be paid in US Dollars.

CSP-9.7. India

Section Effective Date: 10-Jan-2015

Pursuant to Condition 34.19 of LevelBlue's India License Agreement for the Provision of Internet Services ("License"), by using Service, the Customer has read and agrees that Customer and all of its Users will comply with the following terms and conditions, if and when applicable:

- Customer shall not misuse the Service by terminating or interconnecting at either end to the Public Switched Telephone Network ("PSTN") or Public Land Mobile Network ("PLMN") (License Conditions 2.2 (v), 34.17).

- Customer shall be bound by any and all orders, directions, regulations and guidelines issued pursuant to any and all India local laws (including but not limited to the statutory provisions and rules of the Indian Wireless Telegraphy Act, 1933, the Telecom Regulatory Authority of India Act, 1997, the Information Technology Act, 2000, the India Penal Code and the ISP License Agreement, as amended from time to time ("Local India Laws")). Customer shall furnish to the Department of Telecommunications ("DOT") and/or the Telecom Regulatory Authority of India ("TRAI"), on demand and in the manner and within the required time frames as may be prescribed from time to time, all such relevant documents and/or information in accordance with those orders, directions, regulations, and guidelines (License Conditions 9.1).
- Customer shall fully cooperate with the DOT, TRAI and/or any Law Enforcement or Government agencies ("appropriate India Government Agency [or Agencies]") in their lawfully authorized investigations (License Conditions 33.7, 34.1).
- Customer shall not transmit any offensive, abusive, indecent, obscene, or other prohibited content, messages or communications using the Service including any content, messages or communications that infringes copyright, intellectual property right or international and/or domestic India Cyber Laws. In the event specific instances of such activities are reported to the Customer by LevelBlue, on the basis of information received by it from any appropriate India Government Agency, the Customer shall cease transmission immediately and prevent the future carriage of such material (License Conditions 33.3, 33.6).
- Customer shall not use the Service for anti-national activities, including but not limited to activities against the public interest, public order, national harmony, or any offenses punishable under the India Penal Code (License Condition 33.7).
- If Customer uses any encryption equipment and/or software higher than 40-bit key length in the symmetric key algorithms or its equivalent in other algorithms, it will require the prior evaluation and approval from the appropriate India Government Agency. Upon approval, the Customer shall deposit the decryption key, split into two parts, with the DOT and shall submit a copy of the DOT approval to LevelBlue (License Condition 2.2 (vii)).
- Customer shall not resell the Service.

CSP-9.8. Mexico

CSP-9.8.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

Invoices shall be rendered in US Dollars and charges shall be paid in US Dollars or its equivalent amount in Mexican Pesos, using the exchange rate published in the "Diario Oficial de la Federación" the same day payment is made.

CSP-9.9. Netherlands Antilles

CSP-9.9.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

Invoices shall be rendered in US Dollars and charges shall be paid in US Dollars.

CSP-9.10. Peru

CSP-9.10.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

LevelBlue will invoice all applicable charges in US Dollars, and Customer shall pay all charges in US Dollars. If any law, rule, or regulation of a competent Peruvian authority requires that payment for services rendered in Peru must be made in Nuevo Soles, the invoice will include the equivalent amount in Nuevo Soles based on the official exchange rate of the Banco Central de la Reserva del Peru on the day immediately prior to the invoice date.

CSP-9.11. Venezuela

CSP-9.11.1. Billing and Payment Currency

Section Effective Date: 09-Jan-2015

Unless otherwise mandated by Venezuelan law, invoices for all applicable charges shall be rendered in US Dollars, and payment shall be made in US Dollars. If any law, rule, or regulation of a competent Venezuelan authority requires that payment for services rendered in Venezuela must be made in Bolivares, payment shall be made at the

exchange rate published by the Banco Central de Venezuela the day before the payment is made.

CSP-10. LevelBlue TMLA Country-Specific Provisions

Section Effective Date: 06-Jun-2016

Except where indicated, the following terms are in addition to the terms stated in the Service Guide.

CSP-10.1. LevelBlue Country-Unique Terms

Section Effective Date: 06-Feb-2015

None.